

CA Network Flow Analysis

Manuel de l'administrateur

9.1.3



La présente documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si (i) un autre accord régissant l'utilisation du logiciel CA mentionné dans la Documentation passé entre vous et CA stipule le contraire ; ou (ii) si un autre accord de confidentialité entre vous et CA stipule le contraire.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2013 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Produits référencés CA

Ce document fait référence aux produits CA suivants :

- CA Infrastructure Management
- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Performance Center
- CA ReporterAnalyzer
- CA Single Sign-On

Documentation connexe

CA fournit une documentation technique complète dans la bibliothèque de CA Network Flow Analysis. Accédez à la bibliothèque en cliquant sur le lien Aide dans l'interface utilisateur de CA Network Flow Analysis.

Les fichiers PDF et HTML des manuels sont disponibles dans la bibliothèque de la documentation. Pour accéder à la bibliothèque, cliquez sur le lien Aide dans l'interface utilisateur de CA Network Flow Analysis ou de CA Performance Center.

La documentation a peut-être été mise à jour depuis sa publication. Pour vous assurer d'être en possession des dernières mises à jour de la documentation, téléchargez la bibliothèque et les fichiers Readme à partir du site de [support de CA](#).

La documentation de CA Network Flow Analysis 9.1.3 inclut les manuels suivants :

- *Aide en ligne* : assistance destinée aux administrateurs et opérateurs, disponible à partir du lien Aide dans l'interface utilisateur
- *Manuel de l'administrateur* : informations sur la configuration et la maintenance de CA Network Flow Analysis
- *Manuel de l'opérateur* : instructions d'utilisation de la console NFA pour créer, afficher et gérer des rapports
- *Manuel d'installation* : procédure d'installation du logiciel et tâches de configuration uniques à effectuer
- *Manuel de mise à niveau* : procédure de mise à niveau du logiciel et tâches de configuration initiales
- *Notes de parution* : récapitulatif d'améliorations apportées à CA Network Flow Analysis, des corrections et des problèmes en cours de résolution.

Les PDF relatifs au produit se trouvent dans le répertoire suivant :

<chemin_installation>\Reporter\NetQoS.ReporterAnalyzer.WebSite\help\<paramètre régional, tel que en_US, zh_CN ou ja_JP>\NFA_Bookshelf\Bookshelf_Files\PDF.

Le produit Adobe Reader est requis pour afficher les fichiers PDF. Vous pouvez le télécharger sur le site <http://get.adobe.com/reader/>.

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse <http://www.ca.com/worldwide>.

Table des matières

Chapitre 1: Introduction à CA Network Flow Analysis 11

CA Network Flow Analysis.....	11
Avis relatifs aux tiers et contrats de licence	11

Chapitre 2: Configuration initiale 13

Authentification unique	13
Configuration de CA Network Flow Analysis pour une utilisation avec CA Performance Center	14
Enregistrement de CA Network Flow Analysis avec CA Performance Center	15
Test des connexions à la source de données	17
Vérification des profils SNMP.....	17
Vérification des domaines IP	22
Configuration de la collecte de flux	25
Vérification de la réception des données	33
Modification du domaine des interfaces et des interfaces virtuelles personnalisées	36
Configuration des interruptions.....	37
Configuration des comptes d'utilisateurs	38
Configuration des groupes	49
Résultats de l'annulation de l'enregistrement	51
Tâches de post-installation	52
Configuration des interfaces virtuelles personnalisées	54
Configuration des interfaces virtuelles personnalisées	55
Priorités des interfaces virtuelles personnalisées.....	56
Exemple de définitions d'interfaces virtuelles personnalisées	56
Configuration du clonage de paquets	57
Configuration requise pour l'installation de l'outil de clonage de flux	57
Installation de l'outil de clonage de flux	58
Configuration de l'outil de clonage de paquets de flux	58
Restrictions relatives aux paquets clonés	60

Chapitre 3: Administration de CA Network Flow Analysis 61

Page d'administration	61
Menu Interfaces	62
Menu Alertes.....	62
Définir une application : sous-menu Groupes	63
Administration : sous-menu Génération de rapports	63
Administration : sous-menu Authentification.....	64

Administration : sous-menu Système	64
Administration : menu Intégrité	65
Menu A propos de.....	65
Affichage des interfaces physiques et virtuelles	66
Examen des options de la page Interfaces actives.....	66
Recherche de routeur, d'interface ou d'interface virtuelle personnalisée	69
Modification des détails d'un routeur, d'une interface ou d'une interface virtuelle personnalisée	70
Suppression d'un routeur.....	71
Personnalisation de la page Interfaces actives	72
Utilisation des composants de collecte.....	73
Ajout et suppression de Harvesters	74
Modification des détails de composant de collecte.....	75

Chapitre 4: Personnalisation de CA Network Flow Analysis 77

Introduction à la personnalisation	77
Utilisation des groupes et des cumuls d'interface	78
Création de cumuls d'interface	79
Modification d'un cumul d'interface.....	80
Modification de plusieurs cumuls d'interface	81
Suppression de cumuls d'interface	82
Définition des modèles pour les noms d'interfaces et les descriptions	82
Création d'un modèle d'interface personnalisé	83
Modification d'un modèle d'interface	84
Modification du paramètre de l'application pour les noms d'interface	85
Création de groupes de protocoles	86
Création d'un groupe de protocoles de shell.....	87
Configuration du groupe de protocoles	87
Révision des paramètres de groupe de protocoles	89
Etiquetage de valeurs de type de service.....	90
Création et gestion des groupes de types de services	91
Création d'un groupe de types de services de shell.....	91
Ajout de valeurs de types de services au groupe	92
Modification du contenu des groupes de types de service	93
Suppression de groupes de types de service	94
Personnalisation des noms de systèmes autonomes	95
Révision des noms de systèmes autonomes.....	96
Modification de noms de systèmes autonomes	97
Nommage de routeurs	98
Création de filtres de temps.....	99
Création de périodes de génération de rapports.....	101

Chapitre 5: Maintenance de CA Network Flow Analysis 103

Surveillance des composants CA Network Flow Analysis.....	103
Modification des paramètres du service de surveillance	104
Affichage du statut du système	106
Création d'interruptions.....	107
Configuration de destinations des interruptions	110
Configuration des interruptions pour les outils de gestion des pannes externes.....	112
Configuration des interruptions CA Network Flow Analysis pour les outils externes.....	113
Dépannage des problèmes liés aux interruptions intégrées.....	114
Expiration des adresses caduques	114
Gestion des services	116
Journaux de services	118

Chapitre 6: Administration avancée 121

Mappage d'applications	121
Priorités de mappage	122
Configuration des paramètres globaux pour le mappage d'applications	122
Création d'une règle de mappage d'applications de sous-réseau	124
Création d'une règle de mappage d'applications d'hôte	125
Création d'une règle de mappage d'applications Tout (type de service).....	126
Modification de règles de mappage d'applications	127
Suppression de règles de mappage d'applications	128
Utilisation des places réservées	128
Création de règles de places réservées.....	129
Modification de règles de places réservées	130
Suppression de règles de places réservées.....	130
Utilisation des interfaces.....	131
Fusion d'interfaces	132
Activer les interfaces	133
Suppression et désactivation des interfaces.....	134
Modification d'adresses IP de DSA.....	136
Modification de l'adresse IP d'un DSA actuellement connectée	137
Modification de l'adresse IP d'un nouveau DSA	138

Chapitre 7: Analyse et maintenance des données collectées 141

Collecte de données	141
Procédure de collecte des données dans un déploiement à 2 niveaux.....	142
Procédure de collecte des données dans un déploiement à 3 niveaux	143
Données de la présentation de l'entreprise.....	144
Données de résolution en 15 minutes	145

Données de résolution en 1 minute.....	147
Sauvegarde et restauration des données de CA Network Flow Analysis	148
Bases de données à sauvegarder	150
Arrêt des services.....	153
Sauvegarde des bases de données	155
Restauration des bases de données.....	157
Recommandations liées à la préservation de l'intégrité des données.....	158
Glossaire	159
Index	167

Chapitre 1: Introduction à CA Network Flow Analysis

Ce chapitre traite des sujets suivants :

[CA Network Flow Analysis](#) (page 11)

[Avis relatifs aux tiers et contrats de licence](#) (page 11)

CA Network Flow Analysis

CA Network Flow Analysis vous fournit une analyse du trafic réseau avec une visibilité en temps réel du trafic réseau de votre entreprise. Vous pouvez accéder aux données de flux de votre réseau pour une année entière.

Lorsque vous ajoutez CA Network Flow Analysis comme source de données dans CA Performance Center, vous pouvez accéder à CA Performance Center à partir de la console NFA. Vous pouvez comparer les données collectées à partir de plusieurs sources dans CA Performance Center.

Certaines tâches d'administration sont effectuées dans CA Performance Center : gestion des utilisateurs, des rôles, des autorisations, des profils SNMP et de certains types de groupes. Installez CA Performance Center et enregistrez CA Network Flow Analysis comme source de données pour utiliser toutes les fonctionnalités de CA Network Flow Analysis.

Vous pouvez personnaliser les vues dans CA Performance Center, comme décrit dans le manuel *CA Performance Center Administrator and User Guide* (*manuel de l'administrateur et de l'utilisateur de CA Performance Center*).

Avis relatifs aux tiers et contrats de licence

Des logiciels tiers sont intégrés dans CA Network Flow Analysis. Tous les logiciels tiers ont été utilisés en accord avec les termes et conditions pour l'utilisation, la reproduction et la distribution, tels que définis par les contrats de licence applicables.

Les informations concernant les contrats de licence tiers sont fournies dans le document suivant, installé automatiquement avec le logiciel CA Network Flow Analysis :

<chemin_installation>\ThirdPartyContent\ThirdPartyLicenseInfo

Chapitre 2: Configuration initiale

Une fois le logiciel CA Network Flow Analysis installé, des opérations supplémentaires de configuration sont requises. Les rubriques suivantes contiennent les informations qui vous permettront de configurer CA Network Flow Analysis initialement.

Remarque : Ce manuel décrit plusieurs tâches à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure pour ces tâches sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Ce chapitre traite des sujets suivants :

[Authentification unique](#) (page 13)

[Configuration de CA Network Flow Analysis pour une utilisation avec CA Performance Center](#) (page 14)

[Tâches de post-installation](#) (page 52)

[Configuration des interfaces virtuelles personnalisées](#) (page 54)

[Configuration du clonage de paquets](#) (page 57)

Authentification unique

L'outil Authentification unique vous authentifie lors du démarrage pour que vous puissiez vous connecter une fois et utiliser plusieurs produits liés sans devoir vous reconnecter à chaque fois. Si vous vous connectez à CA Performance Center, par exemple, vous pouvez accéder aux informations de CA Network Flow Analysis sans devoir vous connecter à nouveau.

Authentification unique est installé automatiquement lorsque vous installez CA Network Flow Analysis. Pour plus d'informations, reportez-vous au manuel de *CA Single Sign-on*, disponible sur le site du CA Support : <http://support.ca.com>.

Remarque : L'outil Authentification unique utilise le protocole LDAP, s'il est configuré. L'outil Authentification unique n'utilise pas le protocole LDAP par défaut. Si vous effectuez une mise à niveau à partir de CA ReporterAnalyzer NetQoS 9.0.1, mettez à jour toute configuration LDAP d'authentification unique précédente dont vous disposez.

Configuration de CA Network Flow Analysis pour une utilisation avec CA Performance Center

Pour effectuer des tâches d'administration essentielles, CA Network Flow Analysis doit être enregistré dans CA Performance Center ou CA NetQoS Performance Center.

Une fois CA Network Flow Analysis enregistré et les tâches d'administration requises réalisées, les opérateurs pourront afficher des rapports explicites dans CA Network Flow Analysis et dans CA Performance Center.

Pour configurer CA Network Flow Analysis, vous devez effectuer les tâches suivantes :

- Enregistrez CA Network Flow Analysis comme source de données dans CA Performance Center ou CA NetQoS Performance Center.
- Configurez les éléments suivants dans CA Performance Center ou CA NetQoS Performance Center :
 - Profils SNMP
 - Domaines IP
 - Comptes d'utilisateurs, autorisations et rôles
 - Groupes
- Ajoutez des composants de collecte.
- (concerne uniquement les architectures à trois niveaux distribués) Ajoutez des DSA.
- Activez les routeurs et les interfaces pour l'exportation des flux.
- Vérifiez que CA Network Flow Analysis reçoit les données des interfaces.

Ces tâches sont décrites dans les sections suivantes.

Remarque : Ce manuel décrit plusieurs tâches à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure pour ces tâches sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Cette section comprend les rubriques suivantes :

[Enregistrement de CA Network Flow Analysis avec CA Performance Center](#) (page 15)
[Test des connexions à la source de données](#) (page 17)
[Vérification des profils SNMP](#) (page 17)
[Vérification des domaines IP](#) (page 22)
[Configuration de la collecte de flux](#) (page 25)
[Vérification de la réception des données](#) (page 33)
[Modification du domaine des interfaces et des interfaces virtuelles personnalisées](#) (page 36)
[Configuration des interruptions](#) (page 37)
[Configuration des comptes d'utilisateurs](#) (page 38)
[Configuration des groupes](#) (page 49)
[Résultats de l'annulation de l'enregistrement](#) (page 51)

Enregistrement de CA Network Flow Analysis avec CA Performance Center

L'enregistrement s'effectue dans la page de gestion des sources de données de la console CA Performance Center.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Remarque : Pour plus d'informations sur le nombre de sources de données prises en charge par une instance unique de CA Performance Center, reportez-vous aux *Notes de parution de CA Performance Center*.

Procédez comme suit :

1. Vérifiez qu'aucune session CA Network Flow Analysis n'est active. Si plusieurs utilisateurs effectuent des opérations d'écriture simultanées dans la base de données, des problèmes peuvent se produire.
2. Connectez-vous à la console CA Performance Center en tant qu'utilisateur avec le rôle Administrateur.

Remarque : Les administrateurs de clients hébergés ne peuvent pas accéder à la page Gérer les sources de données.

3. Cliquez sur Administration, Sources de données.
La page Gérer les sources de données affiche la liste des sources de données enregistrées.
4. Cliquez sur Créer.
La boîte de dialogue Administration des sources de données s'ouvre.

5. Sélectionnez le type de source de données que vous voulez ajouter dans la liste Type de source.

Remarque : Tous les produits CA qui peuvent être enregistrés en tant que sources de données CA Performance Center sont affichés dans la liste Type de source. La liste n'est pas filtrée pour afficher des produits installés.

6. Saisissez le nom d'hôte de la source de données.

Le nom d'hôte est l'adresse IP ou le nom d'hôte DNS du serveur sur lequel la base de données correspondant à cette source de données est installée. Pour un déploiement distribué de CA Network Flow Analysis, fournissez le nom d'hôte de la console NFA.

7. Indiquez le port à utiliser pour contacter CA Network Flow Analysis.

Pour plus d'informations, consultez le manuel *CA Single Sign-On User Guide*.

8. Sélectionnez le protocole à utiliser pour contacter la source de données. Sélectionnez **https** si votre réseau utilise le protocole SSL pour les communications. Vérifiez que vous avez configuré le système correctement avant de sélectionner l'option **https**.

Remarque : Vous pouvez utiliser SSL pour mes communications entre CA Performance Center et les produits de source de données. Pour plus d'informations, consultez le manuel *CA Sign-On User Guide*.

9. (Facultatif) Saisissez un nom d'affichage pour la source de données CA Network Flow Analysis.

Par défaut, le type de source de données et le nom d'hôte sont combinés pour créer le nom d'affichage. Vous pouvez fournir un autre nom. Par exemple, au lieu de NetworkFlowAnalysis@xxx.x.x.xx, vous pouvez nommer la source de données NetworkFlowAnalysis_NewYork.

10. Confirmez si l'adresse de console Web est identique au nom de l'hôte. Si tel n'est pas le cas, procédez comme suit :

- Désélectionnez la case à cocher Mêmes éléments que la source de données.
- Fournissez le nom d'hôte de console Web, le port et le protocole.

11. Cliquez sur Enregistrer.

La liste des sources de données indique les sources de données enregistrées.

Test des connexions à la source de données

Dans la plupart des cas, le statut indique que l'enregistrement de source de données est terminé. Si le statut indique une erreur, utilisez la fonctionnalité de test dans la page Gérer les sources de données.

Le bouton Test lance un test pour confirmer qu'une nouvelle source de données est enregistrée et connectée correctement. Le test recherche la compatibilité des versions et vérifie que la source de données n'est pas enregistrée auprès d'une instance différente du logiciel NetQoS Performance Center.

Si le test échoue, vérifiez que le nom de serveur ou l'adresse IP est correct pour le type source. Pour plus d'informations, voir Echec du test de source de données.

Vérification des profils SNMP

CA Network Flow Analysis envoie des informations SNMP sécurisées à CA Performance Center lors de l'enregistrement. Ces informations sont ensuite transformées en profils SNMP. *Les profils SNMP* sont des définitions qui contiennent les informations nécessaires pour activer des requêtes sécurisées de MIB d'unité à l'aide de SNMP. Les informations de profil sont mises à jour à chaque synchronisation entre CA Performance Center et CA Network Flow Analysis (toutes les cinq minutes).

Pendant l'installation initiale du produit, vous devez vérifier que les profils SNMP affichés dans la page Gérer les profils SNMP de CA Performance Center sont appropriés pour la surveillance de votre environnement.

Affichage de la liste de profils SNMP

Vous pouvez afficher la liste des profils SNMP qui ont déjà été définis. La liste inclut des informations de haut niveau concernant le contenu de chaque profil.

Si aucune définition de client hébergé n'a été créée, les définitions de la liste de profils SNMP sont partagées entre toutes les sources de données enregistrées. L'administrateur global peut afficher une liste des profils SNMP qui ne sont pas associés explicitement à un client hébergé.

Remarque : Les administrateurs de clients hébergés voient uniquement les éléments associés à leur client hébergé.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur avec le rôle Administrateur.
2. Sélectionnez Administration, Paramètres du système, puis cliquez sur Profils SNMP.

La page Gérer les profils SNMP s'ouvre.

Elle affiche la liste actuelle des profils SNMP.

Les informations suivantes sont répertoriées pour chaque profil :

Classer

Détermine l'ordre dans lequel les informations sécurisées contenues dans un profil SNMP sont utilisées pour essayer d'interroger une unité sélectionnée. Si la requête échoue, le profil suivant est utilisé, dans l'ordre de priorité.

Nom du profil

Définit le nom du profil SNMP. Les noms de profil doivent être uniques, ne peuvent pas être dupliqués sur les différentes versions SNMP et ne sont pas sensibles à la casse.

Port

Identifie le port utilisé pour effectuer des connexions SNMP avec des unités associées à ce profil.

Valeur par défaut : UDP 161.

Version SNMP

Spécifie la version de SNMP que le profil utilise. Dans la mesure où SNMPv1 et SNMPv2C sont similaires du point de vue de la sécurité, ils partagent une option unique. SNMPv3 est une option distincte.

Protocole d'authentification

(SNMPv3 uniquement) Spécifie le protocole d'authentification à utiliser pour contacter des unités associées à ce profil. Les algorithmes d'authentification des paquets SNMPv3 suivants sont pris en charge :

- Aucun (n'essayez pas l'authentification)
- MD5 (Résumé de message 5)
- SHA (Algorithme de hachage sécurisé)

Protocole de confidentialité

Identifie le protocole de chiffrement utilisé pour contacter les éventuelles unités associées. Toujours Aucun si aucun protocole d'autorisation n'est en cours d'utilisation.

Utiliser par défaut

Indique si les informations figurant dans ce profil sont utilisées lorsqu'il n'est pas explicitement affecté à une unité. S'il est désactivé (Non), ce profil est exclu de la détection dans des sources de données qui prennent en charge l'exclusion de profils.

Pour effectuer une action dans cette page, sélectionnez un profil, puis cliquez sur un bouton.

Ajout des profils SNMP

Les administrateurs peuvent créer des profils SNMP dans la console CA Performance Center. CA Network Flow Analysis utilise les profils SNMP pour effectuer des demandes de données auprès des unités. Vous pouvez créer des profils pour SNMPv1/v2C ou pour SNMPv3.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur avec le rôle Administrateur.
2. [Accédez à la page Gérer les profils SNMP](#) (page 17).
La page Gérer les profils SNMP affiche la liste actuelle des profils SNMP.
3. Cliquez sur Créer.
La boîte de dialogue Ajouter un profil SNMP s'affiche.
4. Remplissez les champs et modifiez les paramètres par défaut nécessaires. Certains champs s'appliquent uniquement au profil SNMPv3 ou SNMPv1/v2C

Nom du profil

Définit le nom du profil SNMP. Les noms de profil doivent être uniques, ne peuvent pas être dupliqués sur les différentes versions SNMP et ne sont pas sensibles à la casse.

Version SNMP

Spécifie la version de SNMP que le profil utilise. Dans la mesure où SNMPv1 et SNMPv2C sont similaires du point de vue de la sécurité, ils partagent une option unique. SNMPv3 est une option distincte.

Port

(Facultatif pour SNMPv1/v2C) Identifie le port utilisé pour réaliser les connexions SNMP avec les unités associées à ce profil.

Valeur par défaut : UDP 161.

Nom d'utilisateur

(SNMPv3 uniquement) Identifie l'utilisateur pour le profil, dont les clés secrètes ont été utilisées pour authentifier et chiffrer les paquets SNMPv3. Le nom d'utilisateur est une chaîne de caractères.

Nom de communauté

(SNMPv1/v2C seulement) Définit une chaîne sécurisée qui permet à la source de données d'interroger la MIB de l'unité associée. La communauté que vous spécifiez doit fournir un accès en lecture seule à la MIB de l'unité.

Remarque : Dans le profil SNMP par défaut, la communauté est "public".

Vérifier le nom de la communauté

Confirme la chaîne de communauté sécurisée (nom).

Nom du contexte

Spécifie une collection d'informations de gestion accessibles par une entité SNMP. Le nom de contexte est nécessaire pour fournir une identification bout en bout et pour la récupération des données à partir d'un agent SNMPv3. Le nom de contexte est une chaîne d'octets.

Protocole d'authentification

(SNMPv3 uniquement) Spécifie le protocole d'authentification à utiliser pour contacter des unités associées à ce profil. Les algorithmes d'authentification des paquets SNMPv3 suivants sont pris en charge :

- Aucun (n'essayez pas l'authentification)
- MD5 (Résumé de message 5)
- SHA (Algorithme de hachage sécurisé)

Mot de passe d'authentification

(SNMPv3 uniquement) Spécifie le mot de passe pour l'authentification à l'aide de SNMPv3 et du protocole d'authentification sélectionné.

Remarque : Pour les profils SNMP utilisés avec CA Network Flow Analysis, assurez-vous que le mot de passe spécifié comprend huit caractères au minimum. Si le mot de passe ne répond pas à cette exigence, le profil SNMP n'est pas valide et aucune donnée SNMP ne sera renvoyée lorsque le profil SNMP est utilisé pour l'interrogation. Dans ce cas, les noms d'unités, les noms d'interfaces, les vitesses d'interfaces et les données d'utilisation des interfaces sont manquantes pour les interfaces et les unités correspondantes dans les vues, les rapports et les tableaux de bord.

Vérifier le mot de passe d'authentification

Confirme le mot de passe d'authentification.

Protocole de confidentialité

(Facultatif) Spécifie le protocole de chiffrement à utiliser pour des flux de données envoyés aux unités ou aux serveurs associés à ce profil. Pour créer un profil SNMP valide pour l'interrogation CA Network Flow Analysis, sélectionnez l'un des protocoles suivants :

- Aucun (ne pas chiffrer les communications)
- DES
- AES (chiffrement 128 bits)
- Triple DES

Remarque : Si les options AES 192 et AES 256 sont répertoriées, ne les sélectionnez pas, car elles ne sont pas pris en charge par CA Network Flow Analysis. Si le profil SNMP que vous créez n'est pas valide, aucune donnée SNMP n'est renvoyée pour les unités et les interfaces qui l'utilisent. Dans ce cas, les noms d'unités, les noms d'interfaces, les vitesses d'interfaces et les données d'utilisation des interfaces sont manquantes pour les interfaces et les unités correspondantes dans les vues, les rapports et les tableaux de bord de CA Network Flow Analysis et de CA Performance Center.

L'option de protocole de confidentialité est activée uniquement si l'authentification est activée pour ce profil.

Mot de passe de confidentialité

Définit le mot de passe utilisé lors de l'échange des clés de chiffrement. Consultez la remarque pour connaître les configurations de longueurs possibles.

Vérifier le mot de passe de confidentialité

Définit le mot de passe utilisé lors de l'échange des clés de chiffrement.

Utiliser par défaut pour les nouvelles unités

Spécifie si les informations figurant dans ce profil sont utilisées par défaut. CA Performance Center utilise ces informations pour contacter tout nouvel élément détecté à partir du trafic surveillé. S'il échoue, le profil suivant dans l'ordre de priorité est utilisé. Désactivez ce paramètre pour exclure un profil de la détection.

Remarque : Ce paramètre ne s'applique pas aux sources de données de CA Infrastructure Management Data Aggregator.

5. Cliquez sur Enregistrer.
6. Vous revenez à la page Gérer les profils SNMP. Le nouveau profil apparaît dans la liste.

CA Performance Center effectue automatiquement une synchronisation globale pour envoyer les informations de profil à toutes les sources de données enregistrées.

Vérification des domaines IP

Les domaines IP permettent de résoudre des conflits potentiels d'adresse IP. Les identificateurs de domaine indiquent que deux éléments gérés qui apparaissent par ailleurs en tant qu'adresses IP en double sont en fait deux éléments gérés *différents*.

Les domaines IP permettent également à un administrateur global de contrôler les éléments gérés devant être visibles et accessibles par un administrateur ou un utilisateur particulier.

Dans la page Administration de CA Network Flow Analysis, vous pouvez ajouter des interfaces, des interfaces virtuelles personnalisées, des routeurs et des composants de collecte aux domaines personnalisés que vous créez dans CA Performance Center.

Les informations concernant les domaines IP personnalisés sont renvoyées aux sources de données pendant la synchronisation, où elles sont mises à disposition pour utilisation pendant la configuration de la collecte de données. Les définitions de domaine IP sont partagées entre les sources de données enregistrées auprès de la même instance CA Performance Center.

Pendant l'installation initiale du produit, vous devez vérifier que les domaines IP affichés dans la page Gérer les domaines IP de CA Performance Center sont appropriés pour la surveillance de votre environnement.

Affichage de la liste de domaines IP

Les domaines IP sont requis pour surveiller plusieurs environnements dont les adresses IP se chevauchent. Configurez tous les domaines dont vous aurez besoin avant de commencer à envoyer des données de flux à CA Network Flow Analysis.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur avec le rôle Administrateur.
2. Sélectionnez Administration, Paramètres de l'utilisateur, puis Domaines IP.

La page Gérer les domaines IP affiche la liste actuelle des domaines IP.

Si vous n'avez pas créé de domaines IP personnalisés, seul le domaine par défaut s'affiche dans la liste. Ce domaine prédéfini présente le paramètre Nul pour tous les paramètres.

Tout domaine personnalisé que vous avez créé possède des valeurs pour les paramètres suivants :

Nom

Identifie le domaine.

Description

(Facultatif) Décrit cet espace de noms de domaine, par exemple en nommant l'entreprise qui le possède.

Adresse du DNS principal

Adresse IP du serveur de noms principal pour ce domaine.

Port DNS principal

Numéro de port utilisé par le serveur de noms principal

Adresse DNS secondaire

Adresse IP du serveur de noms secondaire pour ce domaine. Peut être la même que l'adresse principale.

Port DNS secondaire

Numéro de port utilisé par le serveur de noms secondaire.

Adresse de proxy DNS

Adresse IP du serveur proxy DNS.

Proxy DNS activé

Indique si l'adresse du proxy est activée pour ce domaine IP.

Ajout de domaines IP personnalisés

Les administrateurs peuvent affecter des Harvesters, des routeurs, des interfaces et des interfaces virtuelles personnalisées à des domaines. Il est recommandé de configurer chaque client hébergé et domaine personnalisé nécessaire avant d'ajouter des Harvesters. Cela permet d'affecter le paramètre client hébergé/domaine correct lors de l'ajout de chaque Harvester.

Une association client hébergé/domaine correcte permet d'assurer la disponibilité des profils SNMP appropriés pour interroger les routeurs de Harvester.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

La configuration des domaines IP appropriés facilite la réalisation des objectifs suivants :

- Affectation du client hébergé et du domaine IP corrects lors de l'ajout d'Harvesters, de sorte que leurs routeurs et leurs interfaces héritent des associations correctes
- Mise à disposition du contenu spécifique uniquement pour les opérateurs qui doivent le surveiller
- Autorisation des Administrateurs à créer des étiquettes de type de service spécifiques au domaine, des groupes de protocoles et des noms de systèmes autonomes dans CA Network Flow Analysis
- Conflits d'adresses IP évités.

Par exemple, supposons qu'un routeur disposant d'une adresse IP unique contienne des interfaces appartenant à différentes entreprises. Les identificateurs de domaine indiquent que les interfaces constituent des éléments gérés différents, même si l'adresse IP est identique.

Le domaine par défaut est créé automatiquement. Le domaine par défaut inclut tous les éléments qui ne sont pas affectés à un domaine personnalisé.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur possédant les droits de rôle administratifs requis.
2. Accédez à la page Gérer les domaines IP.
Elle affiche la liste actuelle des domaines IP.

3. Cliquez sur Créer.

La boîte de dialogue Administration des domaines IP s'ouvre.

4. Fournissez des informations pour les paramètres suivants :

Nom

Identifie le domaine.

Description

(Facultatif) Décrit cet espace de noms de domaine, par exemple en nommant l'entreprise qui le possède.

Adresse du DNS principal

Adresse IP du serveur de noms principal pour ce domaine.

Port DNS principal

Numéro de port utilisé par le serveur de noms principal

Adresse DNS secondaire

Adresse IP du serveur de noms secondaire pour ce domaine. Peut être la même que l'adresse principale.

Port DNS secondaire

Numéro de port utilisé par le serveur de noms secondaire.

5. (Facultatif) Sélectionnez Activer l'adresse de proxy DNS et indiquez l'adresse IP du serveur proxy. Cette étape est requise uniquement si votre réseau se trouve derrière un serveur proxy DNS.
6. Cliquez sur Enregistrer.
Le nouveau domaine IP s'affiche dans la liste.
7. Répétez les étapes comme requis pour ajouter d'autres domaines IP.

Configuration de la collecte de flux

L'étape suivante consiste à configurer les routeurs dans CA Network Flow Analysis et à vérifier qu'ils envoient des données aux composants de collecte.

Une fois que les tâches suivantes sont terminées, la console NFA et la console CA Performance Center peuvent commencer à collecter les flux :

- (Vivement recommandé) [Ajoutez les domaines dont vous avez besoin](#) (page 24).
- [Ajoutez les composants de collecte pour les routeurs](#) (page 26).
- [Configurez les routeurs et les interfaces de façon à ce qu'ils puissent exporter des données de flux](#) (page 29).

Ajout d'un ou de plusieurs Harvesters

Ajoutez un ou plusieurs Harvesters pour permettre le traitement et l'affichage des données.

Condition préalable :

Recommandation : Si ce n'est pas déjà fait, enregistrez CA Network Flow Analysis dans CA Performance Center et configurez des domaines avant d'ajouter un Harvester.

Procédez comme suit :

1. Ouvrez la console NFA et connectez-vous avec des droits d'administrateur. Vous pouvez, par exemple, entrer l'adresse suivante dans un navigateur :
`http://<adresse_IP>/ra/`
Nom d'utilisateur : *admin*
Mot de passe : *admin*
2. Ouvrez la page Composant de collecte.
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Système : composant de collecte.
La page Composant de collecte s'affiche et indique les composants de collecte actuels.
3. Cliquez sur Ajouter.
La boîte de dialogue Ajouter un Harvester s'ouvre.
4. Entrez les informations suivantes :

Adresse IP

Adresse du serveur de Harvester.

Description

Texte identifiant le Harvester et apparaissant dans la table Harvester.

Domaine

Combinaison de client hébergé et domaine parents pour le Harvester et pour chaque routeur et interface récemment activés qui fournissent des données au Harvester.

Les routeurs et leurs interfaces héritent du client hébergé et du domaine du Harvester parent lors de la première exportation des données de flux par les routeurs et de la première génération de flux par les interfaces. Vous pouvez changer le paramètre client hébergé/domaine ultérieurement, mais ce changement affectera uniquement les nouveaux routeurs actifs et leurs interfaces. Les routeurs et les interfaces qui génèrent des flux avant la modification conserveront leur paramètre existant. Pour modifier le paramètre pour des routeurs et des interfaces, vous devez modifier de manière explicite leurs propriétés dans la console NFA.

L'option Domaine est visible uniquement dans les environnements qui contiennent plusieurs domaines.

5. Cliquez sur Enregistrer.

Le nouveau Harvester est ajouté et apparaît dans la liste des Harvesters, dans le cas où le test de connexion pour l'adresse IP a réussi. Si le test de la connexion au service Web échoue, un message d'erreur apparaît.

Le processus habituel prévoit l'ajout d'un ou de plusieurs Harvesters, puis la configuration des interfaces de routeur en vue de l'exportation des flux vers les Harvesters. Si vous configurez les routeurs pour l'exportation des flux vers le Harvester, la console NFA lance immédiatement la collecte des données à partir du nouveau Harvester. Le domaine des routeurs est alors défini lorsque vous ajoutez le Harvester parent.

Remarque : Vérifiez que les Harvesters que vous ajoutez n'ont pas été supprimés de la page du Harvester. Pour ajouter une instance de Harvester dans CA Network Flow Analysis 9.1.3 après l'avoir supprimée, vous devez réimager le serveur d'installation de Harvester et réinstaller le logiciel de Harvester.

Vérification du domaine du Harvester

Vérifiez que tous les Harvesters sont associés au client hébergé et domaine appropriés avant de configurer des routeurs pour l'exportation des données de flux. Si ce n'est pas déjà fait, configurez tout client hébergé et domaine personnalisés nécessaire avant de continuer.

Procédez comme suit :

1. Ouvrez la page Composant de collecte.
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Système : composant de collecte.
La page Composant de collecte s'affiche et indique les composants de collecte actuels.
2. Dans la ligne du Harvester que vous souhaitez modifier, cliquez sur Modifier.
La boîte de dialogue Modifier le Harvester s'ouvre.
3. (Facultatif) Modifiez le paramètre Domaine si nécessaire (combinaison client hébergé/domaine).
Valeur par défaut : client hébergé par défaut\domaine par défaut.
Vous pouvez également modifier l'adresse IP et la description.
Si aucun domaine IP personnalisé n'a été créé, la table Harvester inclut uniquement les colonnes Adresse IP et Description.
4. Lorsque vous avez effectué vos modifications, cliquez sur Enregistrer.
Vos modifications sont enregistrées.

Configuration des routeurs

Activez NetFlow sur chaque routeur CA Network Flow Analysis en effectuant les étapes décrites dans cette rubrique. Vous pouvez configurer les routeurs pour exporter un des protocoles de flux suivants :

- NetFlow v5, v7, v9 et Sampled NetFlow
- sFlow version 5
- Flux IPFIX, Jflow, cFlow et NetStream conformes aux normes NetFlow v5, v7 ou v9.

Remarque : Veillez à configurer le flux de chaque source à exporter vers un seul Harvester. Si le flux d'une source est exporté vers plusieurs Harvesters, divers problèmes surviendront. Si cela se produit, contactez le [Support CA](#) pour obtenir de l'aide pour la récupération.

Procédez comme suit :

1. Sauvegardez la configuration actuelle du routeur.
2. Configurez l'exportation NetFlow pour chaque interface individuellement.
 - a. Définissez la version d'exportation du flux.
 - b. Définissez l'adresse IP source du flux. Cisco recommande de configurer une interface source de bouclage. Les adresses IP d'interfaces autres que des interfaces de bouclage peuvent changer.
 - c. Définissez l'adresse IP de destination du flux et définissez le port de destination sur 9995.

Remarque : Veillez à ce que le paramètre de port de destination corresponde à la valeur harvesterPort dans la table suivante :

<chemin_installation>/MySQL51/data/harvester/parameter_descriptions.MYD.

Si vous avez défini le port de destination sur une valeur autre que le paramètre par défaut (9995), mettez à jour la valeur harvesterPort recherchée. Les valeurs de port doivent correspondre pour que le Harvester puisse recevoir les données de flux.

- d. Définissez le délai d'expiration du flux sur 1 minute.
3. Activez le flux pour chaque interface.
 - NetFlow v5 ou flux compatible avec v5 :
 - Surveillance de plusieurs interfaces sur un routeur : utilisez toutes les entrées et toutes les sorties. Utilisez la même option pour toutes les interfaces. Les valeurs d'entrée et de sortie peuvent varier légèrement à cause des routeurs qui omettent des paquets et des valeurs de types de services changeantes telles que le trafic entre les interfaces.
 - Surveillance d'une seule interface sur un routeur : utiliser les entrées et les sorties. Avec cette option, moins de flux totaux sont générés du routeur au Harvester et la charge sur le réseau et le Harvester est moins élevée.

- NetFlow v9 ou flux compatible avec v9 :

Le Harvester identifie et déduplique plusieurs flux sur un routeur unique, pour vous permettre d'utiliser les entrées et les sorties sur plusieurs interfaces. Cette option peut s'avérer très efficace pour deux ou trois interfaces. Vous pouvez activer les entrées et les sorties pour toutes les interfaces, mais cette configuration peut représenter une charge supplémentaire inutile pour le Harvester.

4. Configurez la persistance de l'index SNMP sur chaque routeur prenant en charge cette fonctionnalité.

Ajout de DSA (déploiement à trois niveaux)

Applicable à : une architecture à trois niveau dans un déploiement distribué (console NFA, Harvester et DSA installés sur des serveurs distincts)

Dans un déploiement d'architecture à trois niveaux, ajoutez un ou plusieurs DSA pour stocker les données de résolution en 15 minutes (historiques). Dans le cas d'un système autonome ou d'une architecture à deux niveaux, n'ajoutez pas de DSA.

Nous vous recommandons d'ajouter au moins un DSA dans les 30 minutes suivant le lancement de la collecte des flux. Pour que les données de résolution en 15 minutes apparaissent dans les rapports, vous devez ajouter un DSA au déploiement à trois niveaux. Les rapports qui affichent une plage horaire supérieure à 2 heures n'affichent aucune donnée.

Remarque : Modifiez l'adresse IP du DSA retiré plutôt que d'ajouter une instance de DSA. Sinon, les routeurs continuent d'envoyer des données au DSA retiré (et ces données n'apparaissent pas dans les rapports). Si vous devez supprimer un DSA, contactez le support CA pour obtenir de l'aide.

Procédez comme suit :

1. Ouvrez la console NFA et connectez-vous avec des droits d'administrateur.
2. Affichez la page DSA dans l'interface utilisateur de la console NFA :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Système : DSA.
La page DSA s'ouvre et affiche la liste des DSA utilisés.
3. Cliquez sur Ajouter.
La boîte de dialogue Ajouter un DSA s'affiche.
4. Indiquez l'adresse IP du serveur de DSA.

5. Cliquez sur Tester la connexion.

Un test de connexion est effectué pour déterminer si le serveur de la console NFA peut contacter le serveur de DSA et vérifier que MySQL est installé. Si le test réussit, le message suivant apparaît : Test réussi.

6. Répondez au résultat du test :

- a. Si le message Test réussi s'ouvre, cliquez sur OK pour le fermer.
- b. Si un message d'erreur apparaît, fermez le message et suivez la procédure décrite dans la rubrique [Dépannage en cas d'ajout de DSA](#) (page 32).

7. Une fois le test terminé, cliquez sur Enregistrer dans la boîte de dialogue Ajouter un DSA.

Le test de connexion est effectué, suivi d'un test permettant de localiser les paramètres de DSA sur le serveur cible.

8. Notez le résultat du test :

- L'absence de message d'erreur indique que les tests ont réussi. Les résultats suivants se produisent :
 - La boîte de dialogue se ferme et le DSA est ajouté à la liste de DSA.
 - Les Harvesters incluent le nouveau DSA dans les destinations pour les nouvelles interfaces activées qui signalent des données de résolution en 15 minutes.
 - La console NFA transfère les paramètres vers le nouveau DSA.
 - Le DSA est configuré pour récupérer les fichiers de données de résolution en 15 minutes de la console NFA.
 - Les données du DSA apparaissent dans les rapports dans un délai de 30 minutes.
- Si un message d'erreur apparaît, fermez le message et suivez la procédure décrite dans la rubrique [Dépannage en cas d'ajout de DSA](#) (page 32).

Remarques :

- Si un DSA ne commence pas la collecte des données de résolution en 15 minutes dans un délai de 30 minutes après le début de la collecte des flux, des problèmes peuvent se produire. Les données traitées s'accumulent sur le serveur de la console NFA et le traitement est ralenti. Si le problème persiste, la console NFA ne collecte plus les données de résolution en 15 minutes et les données non traitées s'accumulent sur les Harvesters. Si les interruptions de l'outil de surveillance sont configurées, l'outil envoie des alertes indiquant un retard du Harvester ou du Reaper. Si le problème n'est pas résolu, l'exécution des services CA Network Flow Analysis sur les Harvesters peut s'interrompre.

- Chaque DSA est activé pour collecter des données pour un maximum de 5 000 interfaces activées ayant signalé des données.
- Pour plus d'informations sur les types de données, la durée du stockage, les seuils minimum et les types de rapports pour les données de résolution en 15 minutes stockées sur des serveurs de DSA, consultez la rubrique [Données de résolution en 15 minutes](#) (page 145) du *Manuel de l'administrateur de CA Network Flow Analysis*.

Dépannage en cas d'ajout de DSA

Applicable à : une architecture à trois niveau dans un déploiement distribué (console NFA, Harvester et DSA installés sur des serveurs distincts)

Si un des messages d'erreur suivants apparaît lorsque vous cliquez sur Tester la connexion ou sur Enregistrer dans la boîte de dialogue Ajouter un DSA, fermez le message d'erreur et suivez la procédure décrite.

Erreurs de test de connexion

Utilisez les conseils suivants pour corriger les erreurs qui peuvent apparaître lorsque vous cliquez sur Tester la connexion dans la boîte de dialogue Ajouter un DSA.

- L'adresse IP de serveur spécifiée n'est pas valide :
Vous avez entré un format d'adresse IP non valide. Vérifiez que l'adresse IP entrée est correcte.
- "System.Web.Services.Protocols.SoapException...":
Vérifiez que le service NetQoS MySql51 s'exécute sur le serveur de la console NFA. Si le service n'est pas en cours d'exécution, démarrez-le.
- Unable to connect to any of the specified MySQL hosts (la connexion à un des hôtes MySQL spécifiés est impossible) :
Démarrez le service NetQoS MySql51 sur le serveur du DSA. Vérifiez que le service NetQoS MySql51 s'exécute sur le serveur du DSA. Si le service n'est pas en cours d'exécution, démarrez-le.
- Unknown database nqrptr (base de données nqrptr inconnue) :
La base de données de DSA nqrptr n'a pas été trouvée sur le serveur cible. Vérifiez que l'installation du logiciel DSA est terminée.

Erreurs d'enregistrement

Utilisez les conseils suivants pour corriger les erreurs qui peuvent apparaître lorsque vous cliquez sur Enregistrer dans la boîte de dialogue Ajouter un DSA.

- Un enregistrement existant est déjà en cours d'utilisation :
Entrez l'adresse IP d'un DSA qui n'est pas déjà dans la liste de DSA.

- Connection must be valid and open (la connexion doit être valide et ouverte) :
Vérifiez que le service NetQoS MySQL51 s'exécute sur le serveur du DSA. Si le service n'est pas en cours d'exécution, démarrez-le.
- "System.Web.Services.Protocols.SoapException...":
Vérifiez que le serveur cible s'exécute et est accessible par le serveur de la console NFA. Vérifiez que le service NetQoS MySQL51 s'exécute sur le serveur de la console NFA. Si le service n'est pas en cours d'exécution, démarrez-le.
- Table 'nqrptr.settings' doesn't exist (la table nqrptr.settings n'existe pas)
La table de paramètres de DSA n'a pas été trouvée. Le logiciel de DSA n'a pas été installé correctement sur le serveur cible.
 - Vérifiez que vous avez entré l'adresse IP correcte pour le DSA (et non l'adresse IP d'un Harvester ou de la console NFA).
 - Vérifiez que l'installation du logiciel DSA est terminée.

Vérification de la réception des données

Pour vérifier que les données sont reçues, effectuez les tâches suivantes :

- [Vérification de l'activation des interfaces](#) (page 34)
- [Vérification de la visibilité des interfaces dans la console NFA](#) (page 35)

Vérification de l'activation des interfaces

Une fois que vous avez configuré CA Network Flow Analysis pour la réception des données de flux, déterminez quelles sont les interfaces surveillées.

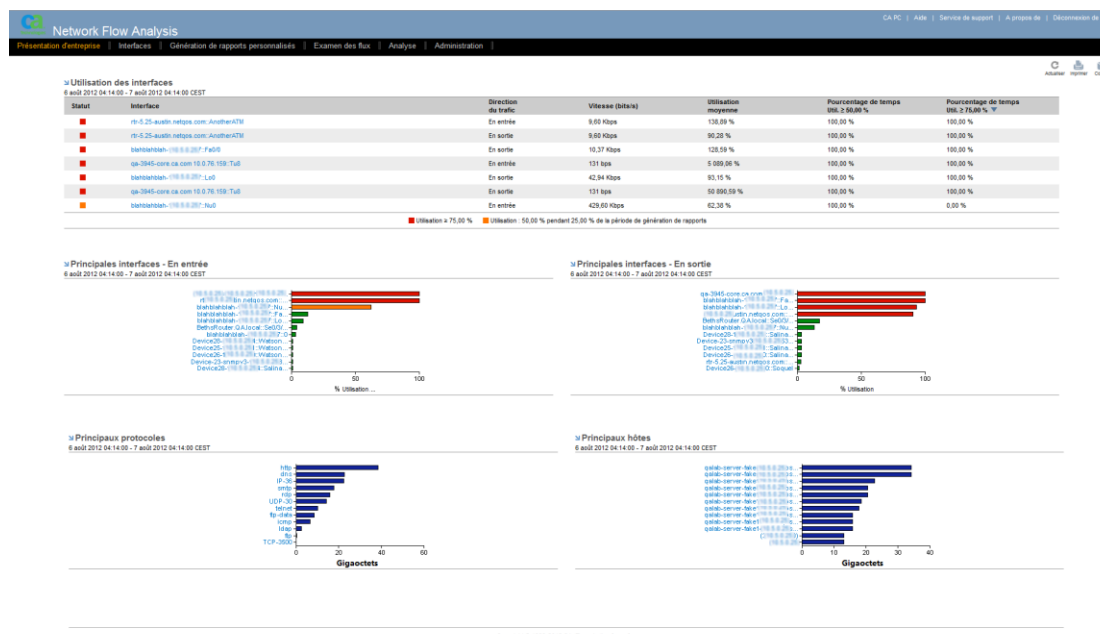
Procédez comme suit :

1. Ouvrez la console NFA et connectez-vous avec des droits d'administrateur.
2. Ouvrez la page Interfaces disponibles :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Système : Activer.
La page Available Interfaces s'ouvre.
3. Pour afficher la liste d'interfaces, cliquez sur la flèche à gauche du nom du routeur pour développer les détails du routeur.
4. Examinez la liste pour savoir quelles interfaces sont activées.
5. Pour modifier le statut d'une interface, activez la case à cocher à côté d'une ou de plusieurs interfaces, puis cliquez sur Activer ou Désactiver.
Les interfaces sélectionnées sont activées ou désactivées.
6. Répétez ces étapes pour chaque routeur.

Vérification de la visibilité des interfaces dans la console NFA

Vérifiez que les interfaces s'affichent dans la console NFA.

1. Vérifiez que les interfaces sont visibles dans la page Présentation d'entreprise :
 - a. Connectez-vous à la console NFA.
 - b. Cliquez sur Présentation d'entreprise dans le menu principal.
 - c. Vérifiez que les vues de rapport affichent les interfaces.



2. Vérifiez que les interfaces sont visibles dans Interface Index :
 - a. Dans le menu de la console NFA, cliquez sur Interfaces.
L'index d'interface s'ouvre.
 - b. Vérifiez qu'il inclut les interfaces que vous pensiez y trouver.
Vous pouvez développer les détails du routeur pour en afficher les interfaces. Vous pouvez également utiliser la zone de recherche et entrer un nom entier ou partiel ou une description pour rechercher des routeurs ou des interfaces.
3. Si les interfaces ne s'affichent pas dans la console NFA, effectuez la procédure de dépannage préliminaire suivante :
 - Vérifiez que les services CA Network Flow Analysis sont en cours d'exécution sur le serveur de la console NFA.
 - Réviser les journaux. Affichez les journaux dans la console NFA ou ouvrez-les à partir du répertoire `<répertoire_installation_NFA>\reporter\Logs`.

Modification du domaine des interfaces et des interfaces virtuelles personnalisées

Les interfaces et les interfaces virtuelles personnalisées héritent leur paramètre de domaine/client hébergé initial du routeur et du Harvester parents. Le paramètre est hérité lorsque le Harvester parent est ajouté et lors de la première activation du routeur et des interfaces. Si le Harvester n'est associé à aucun domaine personnalisé, les routeurs et les interfaces sont affectés au domaine par défaut lors de leur activation.

Vous pouvez modifier les paramètres des interfaces et des interfaces virtuelles personnalisées pour les associer à un client hébergé et un domaine à tout moment. Le paramètre ne doit pas nécessairement correspondre au routeur ou à l'Harvester parent.

La modification de ce paramètre peut affecter les opérateurs ayant accès aux données de l'interface. Le paramètre n'affecte pas les profils SNMP utilisés pour l'interrogation. Le client hébergé du routeur détermine l'ensemble de profils SNMP à interroger.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.
La page Interfaces actives s'ouvre et indique les routeurs actuels et leurs interfaces actives.
2. Recherchez et sélectionnez la case à cocher située près de l'une ou de plusieurs interfaces que vous voulez associer à un client hébergé et un domaine.
 - Pour rechercher des routeurs parents, des interfaces ou des interfaces virtuelles personnalisées, entrez tout ou partie de l'adresse IP de routeur, du nom de routeur ou d'interface, ou de la description d'interface dans le champ Rechercher, puis cliquez sur Rechercher. Développez les détails du routeur.
 - Pour accéder à une interface ou à une interface virtuelle personnalisée manuellement, allez à la page qui contient le routeur parent et cliquez sur la flèche à côté du nom du routeur. Les détails du routeur s'étendent et indiquent les interfaces et les interfaces virtuelles personnalisées.
3. Cliquez sur Modifier.
La boîte de dialogue de modification s'affiche. La liste de sélection Domaine figure dans la boîte de dialogue uniquement s'il existe plusieurs domaines.
4. Dans la liste Domaine, sélectionnez une option de client hébergé/domaine.

5. Cliquez sur Enregistrer.

La boîte de dialogue se ferme. Les modifications sont reflétées dans la page Interfaces actives.

Remarque : Vous pouvez également modifier le paramètre du domaine/client hébergé des [Harvesters](#) (page 75) et des [routeurs](#) (page 70).

Configuration des interruptions

L'étape suivante consiste à configurer les paramètres d'interruption dans CA Network Flow Analysis, à vérifier que CA Performance Center reçoit les événements à partir des interruptions et à configurer des courriels de notification pour les événements.

Pour terminer la configuration des interruptions, effectuez les tâches suivantes :

- Configurez la destination des interruptions dans la console NFA :
 - Pour les interruptions de l'outil de surveillance, utilisez la page Paramètres de l'outil de surveillance.
 - Pour les interruptions du Reaper, utilisez la page Paramètres de l'application.
- Créez les interruptions dont vous avez besoin. Consultez la rubrique Création d'interruptions du *Manuel de l'administrateur CA Network Flow Analysis*.
- Synchronisez de nouveau CA Network Flow Analysis dans la page Gérer les sources de données de CA Performance Center.
- (Facultatif) Consultez les fichiers journaux pour vérifier que les événements ont été générés et envoyés au gestionnaire d'événements.
- Vérifiez que les événements sont affichés dans la page Affichage des événements de CA Performance Center.
- (Facultatif) Si la page Affichage des événements n'indique pas les événements comme prévu, vérifiez que le nom d'hôte du gestionnaire d'événements peut être résolu par le serveur DNS pour CA Network Flow Analysis.
- (Facultatif) Configurez les courriels de notification pour les événements qui vous intéressent.

Configuration des comptes d'utilisateurs

Un compte d'utilisateur prédéfini (admin) est inclus avec l'installation de CA Network Flow Analysis. Le compte admin possède des droits d'administration complets.

L'administrateur de CA Performance Center doit créer un compte d'utilisateur pour chaque personne qui utilisera le produit, administrateurs et opérateurs. Les comptes d'utilisateurs personnalisés améliorent la sécurité des produits et bénéficient des droits de rôle strictement définis qui déterminent l'accès des utilisateurs aux différentes fonctionnalités et données des produits.

Il est préférable de déployer les comptes d'utilisateurs personnalisés dans un système planifié de façon appropriée et qui inclut des groupes personnalisés. Les groupes personnalisés sont affectés en tant qu'autorisations pour permettre aux opérateurs du produit d'afficher uniquement les données, menus et tableaux de bord dont ils ont besoin pour effectuer leurs tâches quotidiennes.

Affichage d'une liste des comptes d'utilisateurs

La page Gérer les utilisateurs de la console CA Performance Center vous permet d'afficher les paramètres de haut niveau pour les comptes d'utilisateurs.

Avant de créer des comptes d'utilisateurs personnalisés, seuls deux comptes d'utilisateurs prédéfinis sont disponibles.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur disposant des droits de rôle d'administration requis.
2. Cliquez sur Administration, Paramètres de l'utilisateur et Utilisateurs.

La page Gérer les utilisateurs s'ouvre. Cette page s'affiche la liste actuelle des comptes d'utilisateurs.

La table inclut les informations suivantes concernant chaque compte d'utilisateur :

User Name

Nom de connexion pour le compte d'utilisateur.

Rôle

Rôle affecté au compte d'utilisateur.

Droit CAPC

Identifie le niveau d'accès aux sources de données enregistrées dans CA Performance Center.

Autorisation

Répertorie les groupes d'autorisations affectés à ce compte. Les groupes d'autorisation apparaissent comme des emplacements imbriqués dans l'arborescence Groupes.

Par défaut : /Tous les groupes.

Status

Indique si le compte d'utilisateur est activé ou désactivé.

Pour effectuer une action sur cette page, cliquez sur l'un des boutons du bas.

Ajout de comptes d'utilisateurs

Ajoutez un compte d'utilisateur pour chaque personne qui utilisera CA Network Flow Analysis et CA Performance Center. A des fins de sécurité, les comptes d'utilisateurs ne devraient pas être partagés.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Remarque : Avant de créer un compte d'utilisateur, confirmez que les rôles et les groupes requis existent.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur avec les droits de rôle d'administration requis.
2. Accédez à la page Gérer les utilisateurs.
Elle affiche la liste actuelle des comptes d'utilisateurs.
3. Cliquez sur Nouveau.
L'assistant Créer un utilisateur s'ouvre.
4. Entrez des informations pour les paramètres suivants :

User Name

Nom de connexion pour le compte d'utilisateur. Limité à 50 caractères.

Description

(Facultatif) Décrit le compte d'utilisateur pour vous aider à l'identifier.

Adresse électronique

(Facultatif) Associe une adresse électronique au compte d'utilisateur.

Langue préférée

Spécifie la langue parlée par l'opérateur associé au compte d'utilisateur.

Type d'authentification

Identifie la méthode d'authentification qui s'applique à ce compte d'utilisateur. La méthode doit correspondre à la configuration de l'authentification unique. Sélectionnez l'une des options ci-dessous.

- Performance Center : le schéma d'authentification par défaut déployé par CA Performance Center.
- Externe : un schéma d'authentification tiers, comme LDAP ou SAML.

Mot de passe

Définit un mot de passe pour le compte d'utilisateur. Le mot de passe est limité à 32 caractères.

Fuseau horaire

Correspond au fuseau horaire dans lequel l'utilisateur affichera des données.

Par défaut : UTC (Temps universel coordonné).

Rôle

Rôle affecté au compte d'utilisateur.

Etat du compte

Détermine si le compte est activé pour l'utilisation (activé).

5. Cliquez sur Groupes d'autorisations.

L'assistant avance jusqu'à la boîte de dialogue suivante.

6. Ajoutez des groupes d'autorisations au compte d'utilisateur, comme suit :

- Développez les groupes dans l'arborescence Groupes disponibles sur la gauche pour que les sous-groupes s'affichent.
- Sélectionnez un groupe ou un sous-groupe.
- Cliquez pour l'ajouter à la liste Groupes sélectionnés à droite.
- Répétez cette opération si nécessaire.

Les groupes d'autorisations sélectionnés s'affichent dans le volet Groupes sélectionnés.

Un groupe par défaut a été automatiquement sélectionné pour l'utilisateur.

7. Sélectionnez un autre groupe dans la liste déroulante Groupe par défaut.
Lorsque l'utilisateur se connecte, les données provenant du groupe par défaut s'affichent dans des tableaux de bord par défaut.
8. Cliquez sur Droits de produit pour passer à la boîte de dialogue suivante de l'assistant.
9. Cliquez sur les valeurs affichées dans la colonne Droits du produit pour activer des listes déroulantes.



Chaque source de données enregistrée comporte une liste distincte.

Sélectionnez l'un des droits du produit suivants dans les listes déroulantes :

Administrateur

Exécute toutes les fonctions, y compris la création et la modification de groupes, de menus, de tableaux de bord, de rôles et de comptes d'utilisateur.

Utilisateur avancé

Crée des menus et des tableaux de bord. Peut également modifier et créer des rôles.

Utilisateur

Affiche les menus et tableaux de bord désignés par un administrateur ou un utilisateur avancé.

Aucun

N'a pas accès à une source de données. Ce paramètre empêche l'utilisateur de suivre un chemin d'accès en profondeur à partir d'une vue dans CA Performance Center jusqu'à l'interface utilisateur de source de données. Par défaut, tous les utilisateurs possèdent ce paramètre de droit du produit pour toutes les sources de données.

Remarque : Le même compte d'utilisateur peut avoir des droits différents pour des sources de données différentes.

10. Cliquez sur Enregistrer.
Le nouveau compte d'utilisateur apparaît dans la page Gérer les utilisateurs.

Droits de rôle

Les droits affectés à chaque rôle déterminent l'accès de l'utilisateur à des tableaux de bord et à des menus. Les droits de rôle contrôlent les types de vue que les utilisateurs peuvent afficher et s'ils peuvent ou non exporter des données et personnaliser des paramètres.

Les administrateurs peuvent accorder des droits supplémentaires à des utilisateurs en modifiant leur rôle. La boîte de dialogue Modifier le rôle répertorie les droits de rôle actuellement affectés aux rôles. La page Gérer les utilisateurs affiche le rôle affecté à chaque utilisateur.

Remarque : Ne supprimez pas les droits de rôle administratifs de votre compte d'administrateur principal. L'accès administratif à la console est requis.

Ajout de droits de rôle pour les utilisateurs

Si les rôles d'utilisateur prédéfinis fournis avec CA Performance Center ne correspondent pas à votre configuration requise, vous pouvez ajouter des rôles d'utilisateur personnalisés. Dans l'idéal, vous créez les rôles dont chaque opérateur de produit unique a besoin pour pouvoir remplir ses responsabilités professionnelles.

Les rôles personnalisés fonctionnent mieux dans un système de groupes personnalisés. Les groupes personnalisés permettent d'accorder précisément un accès aux tableaux de bord et aux fonctionnalités de produit tout en limitant l'accès aux données sensibles. Les mêmes groupes que vous créez pour organiser des données peuvent servir de "groupes d'autorisation" lorsque vous configurez des autorisations de compte d'utilisateur.

Un nouveau rôle n'a pas de droits de rôle jusqu'à ce que vous les ajoutiez.

Ajouter un rôle

Nom: *

Description:

Statut du rôle: *

Interface de produit	Droits du rôle	Description
Définition de menu	-Aucun-	Cliquez sur Modifier pour sélectionner des m...
Performance Center	-Aucun-	Cliquez sur Modifier pour sélectionner des d...
NetworkFlowAnalysis@10.0.14.106	-Aucun-	Cliquez sur Modifier pour sélectionner des d...

Modifier

Enregistrer Enregistrer et poursuivre l'ajout Annuler

Remarque : Lorsque vous avez fini de créer un rôle, vous devez l'affecter à un compte d'utilisateur lors d'une étape distincte. Les rôles deviennent actifs après leur affectation à des comptes d'utilisateurs. Seuls les utilisateurs disposant du rôle Administrer les utilisateurs peuvent affecter des rôles à des comptes d'utilisateurs.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur disposant des droits de rôle d'administration requis.
2. Accédez à la page Gérer les rôles.
Elle affiche la liste actuelle des rôles.
3. Cliquez sur Créer.
La boîte de dialogue Ajouter un rôle s'ouvre.
4. Fournissez les informations requises et faites des sélections dans les champs fournis :

Nom

(Facultatif) Identifie le rôle. Limité à 45 caractères.

Description

(Facultatif) Décrit le rôle. Par exemple, identifie les taxes en rapport avec le travail effectué par l'utilisateur associé.

Activer le rôle

Permet d'activer le rôle. Requis pour donner aux utilisateurs disposant de ce rôle l'accès accordé par des droits de rôle.

5. Sélectionnez Ensemble de menus et cliquez sur Modifier.
La boîte Modifier l'ensemble de menus s'ouvre. Vous pouvez ajouter au rôle des menus répertoriés dans la liste Menus disponibles.
6. Cliquez sur un élément sur la gauche que vous souhaitez ajouter au rôle, puis cliquez sur la flèche droite.
Utilisez les touches Maj + Clic ou Ctrl + Clic pour sélectionner plusieurs éléments dans la liste.
L'élément sélectionné passe dans la liste Menus sélectionnés.

7. (Facultatif) Utilisez les flèches montante et descendante pour déplacer des éléments dans la liste. L'ordre de menus dans la liste détermine leur ordre sur l'onglet Tableaux de bord.
8. Cliquez sur Enregistrer.
Vous revenez à la page Ajouter un rôle.
9. Sélectionnez Performance Center, puis cliquez sur Modifier.
La boîte de dialogue Modifier les droits associés au rôle s'ouvre et vous permet de sélectionner des droits d'accès pour ce rôle. Vous pouvez ajouter au rôle des droits de rôle répertoriés dans la liste Droits disponibles. Pour plus d'informations, consultez la section Droits de rôle.
10. Cliquez sur un élément sur la gauche que vous souhaitez ajouter au rôle, puis cliquez sur la flèche droite.
Le droit d'accès est déplacé dans la liste Droits sélectionnés.
11. (Facultatif) Utilisez les flèches montante et descendante pour déplacer des éléments dans la liste. L'ordre de droits de rôle détermine leur priorité dans des cas où les droits se chevauchent.
12. Cliquez sur Enregistrer.
Vous revenez à la page Ajouter un rôle.
13. Cliquez sur Enregistrer.
Le nouveau rôle est créé et apparaît dans la Liste des rôles.

Affectation de groupes d'autorisations à des comptes d'utilisateurs

Les différents opérateurs de CA Network Flow Analysis et de CA Performance Center requièrent des autorisations d'accès aux données afin de surveiller des données. Les autorisations d'accès sont basées sur des groupes. Vous pouvez affecter des autorisations d'accès en fonction de votre plan pour les groupes personnalisés.

Pour affecter des autorisations, modifiez les comptes d'utilisateurs dans la console CA Performance Center. L'objectif est de s'assurer que tous les opérateurs voient uniquement les données dont ils ont besoin.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Procédez comme suit :

1. Connectez-vous en tant qu'utilisateur disposant de droits d'administrateur.
2. Cliquez sur Administration, Paramètres de l'utilisateur et Utilisateurs.
La page Gérer les utilisateurs s'ouvre.
3. Sélectionnez un compte d'utilisateur à modifier et cliquez sur Modifier.
L'assistant Ajouter un utilisateur s'ouvre.
4. Cliquez sur Groupes d'autorisations.
L'assistant affiche la page Groupes d'autorisations.
5. Ajoutez des groupes d'autorisations au compte d'utilisateur, comme suit :
 - Développez les groupes dans l'arborescence Groupes disponibles sur la gauche pour que les sous-groupes s'affichent.
 - Sélectionnez un groupe ou un sous-groupe.
 - Cliquez sur la flèche droite pour l'ajouter à la liste Groupes sélectionnés à droite.
 - Répétez cette opération si nécessaire.Les groupes d'autorisations sélectionnés s'affichent dans le volet Groupes sélectionnés.
6. Sélectionnez un groupe dans la liste déroulante Groupe par défaut.
Lorsque l'utilisateur se connecte, les données provenant du groupe par défaut s'affichent dans des tableaux de bord par défaut.

7. Cliquez sur Enregistrer.

Les modifications sont enregistrées dans le compte d'utilisateur, et vous revenez à la page Gérer les utilisateurs.

Les groupes personnalisés ont été créés et affectés en tant qu'autorisations au personnel informatique. Lorsque les membres du personnel se connectent à CA Performance Center, ils peuvent afficher des données à partir des systèmes qui leur sont affectés.

Affectation de droits de produit

Chaque source de données enregistrée dans CA Performance Center dispose de ses propres droits de produit, notamment des droits uniques pour l'interface correspondante. Les administrateurs utilisent CA Performance Center pour octroyer des droits de produit aux utilisateurs, pour chaque source de données. Les droits de produit de source de données affecte la capacité des utilisateurs à suivre un chemin d'accès à une vue détaillée à partir d'une vue de données CA Performance Center vers l'interface native pour la source de données. Les droits octroyés de cette manière dépendent de chaque instance de source de données. Par exemple, si plusieurs sources de données CA Network Flow Analysis sont enregistrées dans une instance CA Performance Center, les droits de produit pour chaque console NFA sont affectés séparément.

Le compte d'administrateur par défaut (admin), est verrouillé pour empêcher toute modification des droits du produit. Ce compte requiert des droits d'administrateur pour toutes les sources de données enregistrées. Si vous sélectionnez un groupe de comptes qui inclut le compte d'administrateur, vous ne pouvez pas modifier les droits du produit pour aucun des comptes sélectionnés.

Droits du produit CA Network Flow Analysis

Un utilisateur doit disposer des droits du produit sur la source de données CA Network Flow Analysis pour se connecter à la console NFA. Les droits du produit spécifient également l'accès à la page Administration et à certaines fonctions :

Utilisateur

Permet d'accéder aux rapports sur les principales interfaces et l'utilisation des interfaces dans la page Enterprise Overview (Présentation de l'entreprise).

Un utilisateur avec les paramètres Groupe d'autorisations appropriés peut accéder aux rapports suivants :

- Rapports sur les principaux hôtes et les principaux protocoles dans la page Enterprise Overview (Présentation de l'entreprise)
- Rapports de page d'interfaces
- Rapports existants dans les pages Custom Reporting, Flow Forensics et Analysis

Les paramètres Groupe d'autorisations et Rôle déterminent si l'utilisateur peut exécuter également les rapports existants, créer des rapports et gérer des rapports. Pour créer des rapports, un utilisateur doit avoir accès à tous les groupes.

Utilisateur avancé

Fournit un accès de niveau Utilisateur et les droits accordés par le paramètre Rôle.

Administrateur

Permet d'accéder à la page Administration et à toutes les fonctions, dont les droits de création et de gestion des comptes d'utilisateurs, des rôles, des groupes, des profils SNMP et de planification de rapports.

Configuration des groupes

Nous vous recommandons de créer des groupes personnalisés pour une meilleure gestion des éléments dans les tableaux de bord de CA Performance Center. Des groupes personnalisés sont requis pour permettre aux opérateurs d'afficher des données concernant les performances des routeurs qu'ils gèrent.

Correctement configurés, les groupes peuvent empêcher les opérateurs d'afficher certaines données pour des raisons de sécurité. L'administrateur peut autoriser certains utilisateurs à accéder aux données qui appartiennent à leur zone de responsabilité, à un emplacement ou à sous-réseau physique par exemple.

Création de groupes personnalisés

Avant de commencer à créer des groupes, planifiez une stratégie et une structure. Considérez les types d'autorisations d'accès dont les opérateurs ont besoin pour effectuer leurs tâches de surveillance. Si nécessaire, vous pouvez discuter vos objectifs en termes d'organisation et de surveillance avec un représentant technique CA.

Créez des groupes sous le noeud Tous les groupes dans l'arborescence de groupes, ou dans un groupe de sites ou un groupe personnalisé existant. Vous ne pouvez pas ajouter de groupes à des groupes système qui apparaissent "verrouillés" dans l'arborescence Groupes.

Vous pouvez ajouter au maximum 2000 groupes enfants à un groupe parent.

Remarque : Cette rubrique décrit la procédure à réaliser dans CA Performance Center. Si vous installez CA Network Flow Analysis et que vous l'enregistrez comme source de données pour CA NetQoS Performance Center, la procédure sera légèrement différente. Pour plus d'informations sur les tâches dans CA NetQoS Performance Center, cliquez sur Aide dans la console CA NetQoS Performance Center.

Procédez comme suit :

1. Connectez-vous à la console CA Performance Center en tant qu'utilisateur disposant des droits de rôle d'administration requis.
2. Accédez à la page Gérer les groupes.
La page affiche des groupes actuels dans une arborescence.
3. Développez des noeuds dans l'arborescence de groupes pour trouver un emplacement pour le nouveau groupe.
4. Cliquez avec le bouton droit de la souris sur le noeud, puis sélectionnez Ajouter un groupe.
La fenêtre Ajouter un groupe s'affiche.
L'onglet Créer est sélectionné par défaut.

5. Fournissez des valeurs pour les paramètres suivants :

Nom du groupe

Spécifie un nom pour le groupe. N'utilisez pas les caractères spéciaux suivants dans des noms de groupe : /&\,%.

Description

(Facultatif) Vous aide à identifier le groupe.

6. Confirmez la valeur du paramètre suivant :

Inclure les enfants des éléments gérés

Ajoute automatiquement les enfants des éléments gérés lorsque les éléments sont ajoutés à ce groupe. Si vous désactivez cette option et ajoutez un routeur au groupe, les interfaces sur ce routeur ne sont pas incluses. Par conséquent, leurs données ne sont pas visibles dans des vues de menu d'analyse en profondeur.

Par défaut : Sélectionné.

7. Sélectionnez Personnalisé ou Par site dans la liste de Type de groupe.

Si vous avez sélectionné Par site comme type, un paramètre supplémentaire s'affiche.

8. Indiquez un emplacement dans le champ Emplacement. Le paramètre Emplacement identifie un emplacement physique associé au groupe par site, tel qu'une ville ou une succursale.
9. Cliquez sur Enregistrer.

Le nouveau groupe apparaît dans l'arborescence Groupes.

Il ne contient aucun élément. Deux options sont disponibles pour ajouter des éléments à un groupe personnalisé :

- Remplissez manuellement le groupe en ajoutant des éléments dans l'interface Gérer les groupes.
- Créez des règles pour gérer l'appartenance aux groupes.

Résultats de l'annulation de l'enregistrement

Certaines circonstances requièrent l'annulation de l'enregistrement de CA Network Flow Analysis au niveau de CA Performance Center, par exemple, avant d'enregistrer CA Network Flow Analysis avec une instance CA Performance Center différente. Annulez l'enregistrement de CA Network Flow Analysis dans CA Performance Center uniquement si cela est vraiment nécessaire.

Si vous annulez l'enregistrement de CA Network Flow Analysis, les règles suivantes s'appliquent :

- Utilisateurs : les utilisateurs qui ne sont pas associés à CA Network Flow Analysis sont supprimés. Les ID d'utilisateurs existants sont conservés. Vous ne pouvez pas ajouter de nouveaux utilisateurs ou modifier les paramètres des comptes d'utilisateurs.
- Rôles : les rôles ne sont pas supprimés. Les utilisateurs conservent leurs rôles précédents. Les ID de rôles existants sont conservés. Vous ne pouvez pas modifier les rôles ou les autorisations pour les utilisateurs existants.
- Groupes :
 - les groupes qui n'existent pas dans CA Network Flow Analysis sont supprimés. Vous ne pouvez pas ajouter de groupes ni les modifier.
 - Les groupes imbriqués qui sont associés à une interface sont affichés en tant que groupes d'interfaces dans la console NFA.
 - Les groupes qui ne sont associés à aucune interface apparaissent en tant qu'autorisations.
- Authentification unique et LDAP : l'authentification unique et les valeurs LDAP sont conservées.

Remarque : Pour obtenir une description plus détaillée des résultats d'annulation de l'enregistrement lors d'une mise à niveau de CA Network Flow Analysis, consultez le *Manuel de mise à niveau de CA Network Flow Analysis*.

Tâches de post-installation

Vous pouvez effectuer plusieurs tâches d'administration supplémentaires, selon votre environnement et le nombre d'utilisateurs. Certaines tâches doivent être effectuées dès l'exécution de CA Network Flow Analysis. Considérez les tâches suivantes :

- **Vérification de la configuration des paramètres requis**

Vérifiez que toutes les tâches d'installation sont terminées. Certains paramètres sont requis pour activer certaines fonctionnalités, comme l'envoi de rapports par courriel et le déclenchement des interruptions SNMP.

- **Ajustement des paramètres pour améliorer les performances**

Certains paramètres des rapports peuvent affecter les performances, comme la fréquence de la résolution du nom d'hôte DNS.

- **Vérification des vitesses d'interface**

Si l'utilisation des interfaces dans la console NFA atteint 100 % ou les dépasse (par exemple, comme dans la page Présentation d'entreprise), vous pouvez ajuster les vitesses d'interface. Pour obtenir des informations supplémentaires sur la modification des paramètres d'interface, reportez-vous à la section [Expiration des adresses caduques](#) (page 114).

- **Contrôle de l'affichage de routeur**

Dans un environnement multidomaine, vous pouvez exclure des domaines de l'affichage pour contrôler les routeurs affichés dans la console NFA.

- **Désactivation de la surveillance du trafic généré par les routeurs**

Si vous ne souhaitez pas que les rapports incluent le trafic d'émission pour chaque routeur, définissez le paramètre d'application Pompage de l'émission ou de la multidiffusion sur False.

- **Surveillance de composants de produit**

Les services de surveillance vous permettent de surveiller les composants. Vérifiez que les paramètres appropriés sont configurés pour permettre la notification des problèmes de composant dans les plus brefs délais. Spécifiez des seuils, une adresse électronique pour recevoir des messages et d'autres paramètres. Pour obtenir des informations supplémentaires, reportez-vous à la section [Surveillance des composants de CA Network Flow Analysis](#) (page 103).

- **Ajustement des paramètres de sécurité**

Pour exporter des rapports dans des fichiers CSV, les paramètres de sécurité de votre environnement peuvent rendre nécessaire l'ajout de l'adresse IP de la console NFA à votre liste de sites de confiance.

Remarque : Pour obtenir des informations sur l'installation et la mise à niveau, consultez les manuels suivants :

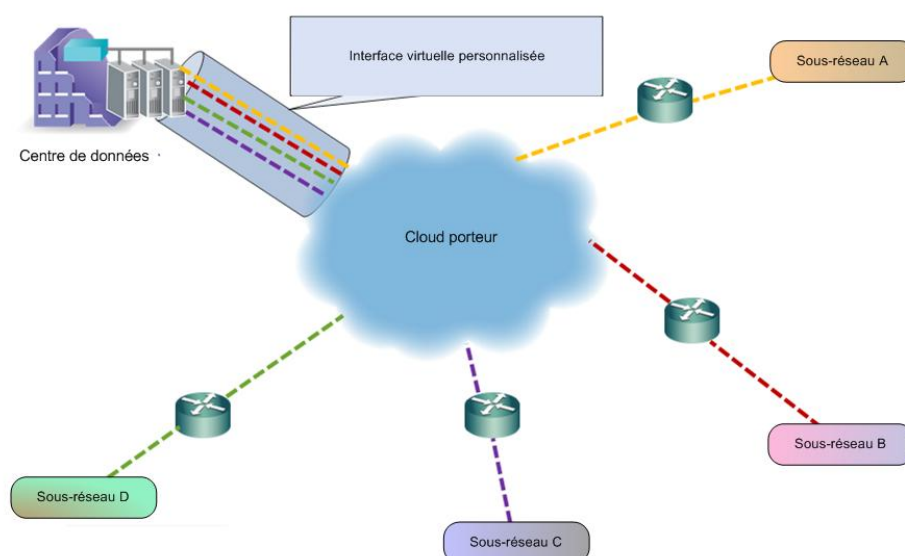
- *Manuel d'installation de CA Network Flow Analysis*
- *Manuel de mise à niveau de CA Network Flow Analysis*

Configuration des interfaces virtuelles personnalisées

Vous pouvez créer des interfaces virtuelles personnalisées pour générer des rapports sur le trafic de sous-réseau. Créez des interfaces virtuelles personnalisées pour un réseau conçu de la façon suivante :

- Le trafic d'un centre de données est transféré aux sous-réseaux à travers un cloud porteur MPLS.
- Le flux est activé sur les routeurs du centre de données plutôt que sur les routeurs à la périphérie du cloud.

Sans interfaces virtuelles, vous ne disposez que d'une visibilité limitée pour identifier les sous-réseaux qui génèrent le trafic pour le cloud porteur. Les interfaces virtuelles vous aident à collecter des données détaillées sur le trafic du sous-réseau dans ce type de configuration.



La définition d'une interface virtuelle personnalisée permet de distinguer le trafic correspondant à une interface du reste du trafic. L'interface virtuelle personnalisée du diagramme distingue le trafic du reste du trafic à l'entrée et à la sortie du centre de données dans le cloud.

Configuration des interfaces virtuelles personnalisées

Créez une interface virtuelle personnalisée pour distinguer le trafic dans une interface et un sous-réseau spécifiques du reste du trafic dans l'interface.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.
La page Interfaces actives s'ouvre et indique les routeurs actuels et leurs interfaces actives.
2. Développez la liste des interfaces pour le routeur parent en cliquant sur la flèche située près du nom du routeur.
3. Sélectionnez la case à cocher située près du nom d'une interface unique.
4. Cliquez sur Ajouter une interface virtuelle personnalisée.
La boîte de dialogue Ajouter une interface virtuelle personnalisée s'ouvre.
5. Saisissez les informations pour les champs suivants :
 - Nom de l'interface : remplacez la valeur par défaut par un nom significatif pour la liste d'interfaces.
Valeur par défaut : nom de l'interface parent, que vous devez remplacer.
 - Description : entrez une chaîne de texte pour faciliter l'identification de l'interface.
 - Vitesse en entrée et vitesse en sortie : identifiez la vitesse de données entrantes dans l'interface parente et sortantes de cette interface.
 - Type : sélectionnez le type d'interface dans la liste.
 - Domaine : sélectionnez un domaine/client hébergé dans la liste ou acceptez le paramètre par défaut.
L'option Domaine est visible uniquement dans les environnements qui contiennent plusieurs domaines.
 - Sous-réseau : entrez une identification de sous-réseau et de masque pour chaque filtre de sous-réseau à utiliser pour l'interface virtuelle personnalisée, puis cliquez sur Ajouter. Utilisez le format suivant :
<adresse_IP_sous-réseau/masque_sous-réseau>
Pour être valides, les interfaces virtuelles personnalisées doivent contenir un ou plusieurs filtres de sous-réseau.

6. Lorsque les paramètres de la boîte de dialogue Ajouter une interface virtuelle personnalisée sont configurés, cliquez sur Enregistrer.

L'interface virtuelle personnalisée est automatiquement déployée dans la minute qui suit. L'icône de classe de la nouvelle interface virtuelle personnalisée la distingue des interfaces physiques.

Important : Si vous supprimez une interface virtuelle personnalisée parente, toutes ses interfaces virtuelles personnalisées enfants seront automatiquement supprimées.

Priorités des interfaces virtuelles personnalisées

Les priorités des interfaces virtuelles personnalisées sont définies selon le degré de spécificité du masque de sous-réseau que vous indiquez. Les masques de sous-réseau de spécificité élevée sont prioritaires. Par exemple, si vous configurez une interface virtuelle personnalisée pour une adresse IP avec un masque de sous-réseau qui correspond à un noeud unique (comme 192.168.20.2/32), la priorité de celle-ci est élevée. Si vous spécifiez une adresse IP avec un masque de sous-réseau qui identifie plusieurs noeuds possibles (comme 192.0.0.0/8), la priorité de l'interface virtuelle personnalisée est faible. La définition de priorités vous permet de faire la distinction entre le trafic des interfaces virtuelles personnalisées vers un hôte d'un sous-réseau étendu et le reste du trafic du sous-réseau.

Remarque : Les rapports qui sont générés pour le trafic entre deux interfaces virtuelles personnalisées avec la même priorité sont parfois incohérents.

Exemple de définitions d'interfaces virtuelles personnalisées

Si vous définissez les interfaces virtuelles personnalisées suivantes :

- CVI-A : 192.168.0.0/16
- CVI-B : 192.168.100.0/24
- CVI-C : 192.168.100.123/32

La génération de rapports suivante est activée :

- CVI-A génère un rapport sur le trafic qui implique le sous-réseau 192.168.x.x, à l'exception du trafic qui implique le sous-réseau 192.168.100.x.
- CVI-B génère un rapport sur le trafic qui implique le sous-réseau 192.168.100.x, à l'exception du trafic qui implique le sous-réseau 192.168.100.123.
- CVI-C génère un rapport sur le trafic qui implique l'hôte 192.168.100.123.

Si vous ajoutez 192.168.100.124/32 en tant que CVI-D, CVI-C ou CVI-D génère un rapport sur le trafic entre 192.168.100.123 et 192.168.100.124. Seule l'une des interfaces virtuelles personnalisées génère des rapports sur le trafic.

Si vous ajoutez 192.168.200.0/24 en tant que CVI-E, CVI-B ou CVI-E génère un rapport sur le trafic entre 192.168.100.x et 192.168.200.x. Seule l'une des interfaces virtuelles personnalisées génère des rapports sur le trafic.

Configuration du clonage de paquets

Vous pouvez utiliser l'outil de clonage de paquets de flux pour cloner des paquets IP à partir d'un routeur NetFlow/IPFIX et les envoyer vers les hôtes de votre choix. L'outil de clonage de paquets de flux est une DLL appelée NFFlowCloneEngine.dll, situé sur le même serveur que Harvester dans le répertoire suivant :
<chemin_installation_NFA>\Netflow\bin.

Configuration requise pour l'installation de l'outil de clonage de flux

Avant d'installer Outil de clonage de flux, vérifiez que votre serveur d'installation satisfait les conditions préalables suivantes :

- Vérifiez que le serveur est configuré et installé ou mis à niveau tel que décrit dans le *Manuel d'installation de CA Network Flow Analysis* ou le *Manuel de mise à niveau de CA Network Flow Analysis*.
- Vérifiez que le serveur contient déjà le logiciel configuré pour fonctionner comme l'un des composants suivants :
 - Serveur de Harvester Windows dans un déploiement CA Network Flow Analysis 9.1.3 distribué
 - Serveur autonome dans un déploiement autonome
- Vérifiez que le serveur dispose de 12.8 Mo minimum d'espace de disque sur le lecteur cible pour Outil de clonage de flux.
- Obtenez le fichier FlowClonerSetup.exe à partir du Support CA et copiez-le à un emplacement sur le serveur d'installation.
- Fermez tous les autres programmes.
- Vérifiez qu'aucun autre utilisateur n'est connecté au serveur.

Installation de l'outil de clonage de flux

Suivez la procédure détaillée dans cette rubrique pour installer Outil de clonage de flux.

Procédez comme suit :

1. Connectez-vous au serveur d'installation en tant qu'utilisateur disposant de droits d'administrateur.

Le serveur d'installation doit contenir le logiciel Harvester CA Network Flow Analysis 9.1.3.
2. Exécutez le fichier FlowClonerSetup.exe. Par exemple, double-cliquez sur le fichier FlowClonerSetup.exe dans l'explorateur Windows.
3. Dans la boîte de dialogue Bienvenue, cliquez sur Suivant.

La fenêtre Récapitulatif de pré-installation s'ouvre et indique le chemin d'installation ainsi que la configuration requise pour l'espace disque. Outil de clonage de flux sera installé dans le même répertoire d'installation racine utilisé pour Harvester ou le logiciel autonome. Le chemin d'installation par défaut est identique à celui du Harvester ou du déploiement autonome CA Network Flow Analysis.
4. Dans la fenêtre Récapitulatif de pré-installation, cliquez sur Installer.

La barre d'état et les messages contextuels affichent la progression de l'installation. La fenêtre Fin de l'installation s'ouvre à l'issue de l'installation.
5. Dans la fenêtre Fin de l'installation, cliquez sur Terminé.

Le programme d'installation se ferme. Un fichier journal d'installation appelé FlowCloner_Install_<horodatage>.log est créé dans le répertoire d'installation racine.

Etape suivante : [modification du fichier de configuration de l'outil de clonage de flux](#) (page 58).

Configuration de l'outil de clonage de paquets de flux

Pour configurer l'outil de clonage de paquets de flux, créez un fichier appelé FlowCloneDef.ini situé dans le même répertoire utilisé pour l'installation de la DLL : <chemin_installation_NFA>\NetFlow\bin. Spécifiez des champs dans l'en-tête et d'autres lignes selon vos besoins en suivant les instructions suivantes :

- *Ligne d'en-tête - Nombre de champs* : la ligne d'en-tête peut contenir au maximum deux champs, mais aucun n'est obligatoire. Si vous ignorez tous les champs dans la ligne d'en-tête, incluez un élément autre qu'un commentaire, par exemple : /utiliser les valeurs par défaut.
- *Ligne d'en-tête - Format* : tous les champs d'en-tête doivent s'afficher sur la même ligne, qui doit être la première ligne non commentée et-remplie dans le fichier.

- *Adresse NIC des paquets clonés* : incluez le champ */retrans ip=* dans la ligne d'en-tête pour spécifier l'adresse IP du NIC (contrôleur d'interface réseau) qui sera utilisé pour envoyer les paquets clonés. Ce champ est facultatif et la valeur par défaut est définie sur la première adresse IP fonctionnelle de l'hôte.

Remarque : Si l'hôte a plusieurs adresses IP, il est vivement recommandé de spécifier l'adresse IP à utiliser.

- *Port de retransmission* : incluez le champ */port=* dans la ligne d'en-tête pour indiquer le port UDP sur lequel les paquets seront retransmis. Ce champ est facultatif et défini par défaut sur le port sur lequel le service Harvester écoute.

Remarque : Il s'agit d'un paramètre global. Les paquets clonés vers les hôtes seront visibles sur le même port.

- *Hôtes de réception des paquets clonés* : pour chaque hôte auquel vous voulez envoyer des paquets clonés, ajoutez une ligne qui commence par le champ */dest ip=*. Fournissez l'adresse IP de l'hôte qui doit recevoir les paquets clonés.
- *Lignes de commentaire* : vous pouvez inclure des lignes de commentaire dans le fichier en plaçant un point-virgule (;) dans la première colonne d'une ligne.
- *Commandes de clonage NetFlow* : pour utiliser la fonctionnalité de clonage NetFlow, utilisez l'une des commandes suivantes :
 - */use defaults* ; acceptez la configuration par défaut et utilisez le premier NIC disponible pour envoyer NetFlow vers le port UDP 9995.
 - */Port=9995* ; utilisez et changez cette valeur pour modifier le port d'exportation de NetFlow. Elle doit figurer sur la première ligne du fichier .ini.

Exemple de fichiers de configuration de clone de flux

Le fichier FlowCloneDef.ini pour un serveur à NIC unique peut être similaire à l'exemple suivant :

```
/use defaults ; take default setup
/dest ip=192.168.0.146send cloned packets to ddev1
/dest ip=192.168.0.144send cloned packets to ddev3
```

Le fichier FlowCloneDef.ini pour un serveur à NIC multiples peut être similaire à l'exemple suivant :

```
/retrans ip=169.254.95.29
/dest ip=192.168.0.144
```

Conventions de fichier de configuration de clone de flux

Lors de création et de la modification du fichier FlowCloneDef.ini, respectez les conventions suivantes :

- *Jetons de valeur* : toutes les valeurs du fichier sont précédées d'un jeton qui les identifie. Ces jetons sont eux-mêmes précédés du caractère | ou /, qui les identifie en tant que tel.

Toute valeur précédée d'un jeton inattendu sera ignorée.

- *Ordre des valeurs* : vous pouvez spécifier des valeurs dans l'ordre de votre choix.
- *Paramètres facultatifs* : vous pouvez ignorer tout paramètre facultatif dans le fichier.
- *Utilisation du point-virgule* :
 - Un point-virgule (;) dans la première colonne d'une ligne permet de commenter la ligne complète.
 - Un point-virgule (;) après un jeton définit l'ensemble du texte jusqu'au démarrage du jeton suivant à ignorer. Cette convention permet de commenter des champs spécifiques. Dans ce cas, le point-virgule ne permet pas de commenter le reste de la ligne.
 - Une séquence de deux points-virgules (;;) permet de tout commenter à partir de ce point jusqu'à la fin de la ligne.

Restrictions relatives aux paquets clonés

Tous les paquets IP clonés possèdent les caractéristiques suivantes :

- Ils sont envoyés avec une valeur de type de service de 0 (zéro), quelle que soit la valeur du paquet d'origine.

Leur port expéditeur est 10 000, quel que soit le port expéditeur du paquet d'origine.

La valeur de leur durée de vie est de 255, quelle que soit la valeur de la durée de vie du paquet d'origine.

- Leur ID de fragment est un numéro arbitraire.

Chapitre 3: Administration de CA Network Flow Analysis

Un administrateur peut utiliser la page Administration de la console NFA pour configurer et personnaliser l'application. Les rubriques suivantes décrivent la page Administration et ses fonctions.

Ce chapitre traite des sujets suivants :

[Page d'administration](#) (page 61)

[Affichage des interfaces physiques et virtuelles](#) (page 66)

[Utilisation des composants de collecte](#) (page 73)

Page d'administration

La page Administration de CA Network Flow Analysis vous permet de consulter, d'administrer et de personnaliser l'affichage des données de réseau. Lorsque vous accédez à cette page, le statut du système s'affiche et les icônes de statut suivantes sont utilisées :

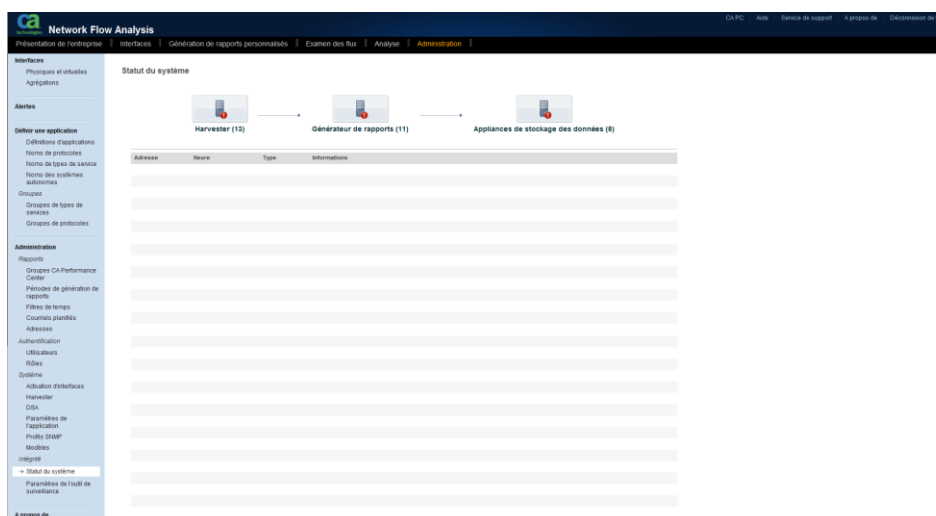
- Coche *verte* : le composant s'exécute sans erreurs.
- Point d'exclamation *rouge* : le composant s'exécute, mais des erreurs sont détectées.

Cliquez sur le point d'exclamation rouge pour afficher le rapport d'erreur correspondant. Le rapport d'erreur inclut l'adresse IP, le type de composant et d'autres d'informations sur l'erreur. Aucun message d'erreur n'est affiché pour la coche verte.

Remarques :

- Pour effectuer des tâches d'administration, connectez-vous avec un compte disposant de droits d'administrateur.
- Le graphique suivant illustre une console NFA enregistrée comme source de données dans CA Performance Center. Si votre console NFA est enregistrée comme source de données dans CA NetQoS Performance Center, certains liens et éléments de menu seront légèrement différents.

Page d'accueil d'administration d'une console NFA enregistrée dans CA Performance Center



Un menu d'options d'administration se trouve sur le côté gauche de la page. La liste suivante décrit la page qui s'ouvre pour chaque option ainsi que sa fonction.

Menu Interfaces

Physique et virtuelle

Affichez le statut des interfaces dans la page Interfaces actives, qui s'ouvre en mode Liste/Modifier. Vous pouvez également modifier, supprimer ou fusionner les interfaces ou créer une interface virtuelle personnalisée.

Cumuls

Cumuler des interfaces dans la page Interfaces de cumul pour afficher les interfaces sous la forme de groupe unifié.

Menu Alertes

Alertes

Ouvrez la page Configuration des interruptions et examinez, ajoutez, modifiez et supprimez des interruptions.

Définir une application : sous-menu Groupes

Définitions d'application

Ouvrez la page Définitions d'applications et définissez des règles de mappage d'applications, des priorités de port, ou des places réservées.

Noms de protocole

Ouvrez la page Configuration du protocole et modifiez un nom de protocole et la description dans le contexte d'un client hébergé et domaine particulier.

Noms ToS

Ouvrez la page Configuration du type de service et modifiez une étiquette de type de service (description) dans le contexte d'un client hébergé et domaine particulier. Vous pouvez en outre ajouter, supprimer, ou modifier des groupes de valeurs de type de service.

Noms AS

Ouvrez la page Noms des systèmes autonomes et recherchez, modifiez, ou réinitialisez les noms des systèmes autonomes dans le contexte d'un client hébergé et domaine particulier.

Groupes de types de service

Ouvrez la page Configuration du groupe de types de service et révisez, ajoutez, supprimez, ou modifiez des groupes de types de service.

Groupes de protocoles

Ouvrez la page Configuration du groupe de protocoles et révisez, ajoutez, supprimez, ou modifiez des groupes de protocoles.

Administration : sous-menu Génération de rapports

Groupes CA Performance Center ou groupes NPC

Dans CA Performance Center ou CA NetQoS Performance Center, ouvrez la page de gestion des groupes. Révisez les groupes système et ajoutez, supprimez, ou modifiez des groupes personnalisés et des groupes par site. Cette option est activée uniquement si CA Network Flow Analysis est enregistré comme source de données dans CA Performance Center ou CA NetQoS Performance Center.

Périodes de génération de rapports

Ouvrez la page Configuration des périodes de génération de rapports. Ajoutez, modifiez et supprimez des périodes de génération de rapports disponibles dans des pages de rapport Interface comme délais pour la période de collecte de données.

Filtres de temps

Affichez, ajoutez, modifiez et supprimez des filtres de temps dans la page Configuration du filtre de temps.

Courriels planifiés

Ouvrez la page Courriels planifiés et révisez les rapports planifiés pour la remise de courriels. Vous pouvez modifier l'adresse de destination, l'objet, le texte du message associé et les options de planification.

Adresses

Ouvrez la page Configuration de l'adresse ou du nom d'hôte et spécifiez un masque et des options de résolution des noms DNS dans le contexte d'un client hébergé et domaine particulier. Répertoirez, modifiez, supprimez et définissez un délai d'expiration pour les adresses. Le délai d'expiration des adresses planifie leur actualisation.

Administration : sous-menu Authentification

Utilisateurs

Ouvrez la page de gestion des utilisateurs dans CA Performance Center ou la page de liste des utilisateurs dans CA NetQoS Performance Center. Révisez les comptes d'utilisateurs existants et leurs paramètres. Ajoutez, supprimez et modifiez des comptes d'utilisateurs. Cette option est activée uniquement si CA Network Flow Analysis est enregistré comme source de données dans CA Performance Center ou CA NetQoS Performance Center.

Rôles

Ouvrez la page de gestion des rôles dans CA Performance Center ou la page de liste des rôles dans CA NetQoS Performance Center. Révisez les noms de rôle existants, les menus disponibles et les fonctionnalités. Ajoutez, supprimez et modifiez des rôles. Cette option est activée uniquement si CA Network Flow Analysis est enregistré comme source de données dans CA Performance Center ou CA NetQoS Performance Center.

Administration : sous-menu Système

Activer les interfaces

Affichez le statut des routeurs sur la page Interfaces disponibles. Affichez la liste et le statut des interfaces pour chaque routeur. Activez, désactivez ou supprimez des interfaces.

Harvester

Ouvrez la page Harvester, puis affichez, ajoutez, modifiez et supprimez les Harvesters qui envoient des données à la console NFA.

**DSA**

Déploiements d'architecture à trois niveaux uniquement : ajoutez un DSA à la configuration ou modifiez l'adresse IP du DSA. Dans un déploiement d'architecture à trois niveaux, un ou plusieurs DSA stockent les données de résolution en 15 minutes (historique) pour les rapports.

Paramètres d'application

Modifiez une série de paramètres d'application à partir de la page Paramètres de l'application.

Profils SNMP

Gérez des profils SNMP dans la page de gestion des profils SNMP dans CA Performance Center ou la liste des profils SNMP dans CA NetQoS Performance Center. Cette option est activée uniquement si CA Network Flow Analysis est enregistré comme source de données dans CA Performance Center ou CA NetQoS Performance Center.

Modèles

Ouvrez la page Modèles d'interface et affichez, ajoutez, modifiez et supprimez des modèles qui déterminent l'affichage des interfaces.

Administration : menu Intégrité

Statut du système

Affichez le statut global des composants CA Network Flow Analysis dans la page Statut du système. Affichez une liste de rapports de problème pour chaque composant.



Le statut des DSA est utile uniquement pour les déploiements d'architecture à trois niveaux. Les DSA ne sont pas incluses dans les déploiements à deux niveaux. Dans un déploiement à deux niveaux, le statut de DSA indique toujours une icône de statut du système verte.

Paramètres de l'outil de surveillance

Affichez et modifiez les paramètres de configuration de l'outil de surveillance à partir de la page Paramètres de l'outil de surveillance.

Menu A propos de

A propos de

Affichez le numéro de version du produit, la date d'installation et la documentation à partir de la page Informations sur la version.

Affichage des interfaces physiques et virtuelles

Les administrateurs peuvent utiliser la page Interfaces actives de la console NFA pour gérer des routeurs et des interfaces.

Cette section comprend les rubriques suivantes :

[Examen des options de la page Interfaces actives](#) (page 66)

[Recherche de routeur, d'interface ou d'interface virtuelle personnalisée](#) (page 69)

[Modification des détails d'un routeur, d'une interface ou d'une interface virtuelle personnalisée](#) (page 70)

[Suppression d'un routeur](#) (page 71)

[Personnalisation de la page Interfaces actives](#) (page 72)

Examen des options de la page Interfaces actives

Utilisez la page Interfaces actives pour afficher et gérer les routeurs, les interfaces et les interfaces virtuelles personnalisées actives.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.
La page Interfaces actives s'ouvre et indique les routeurs actuels et leurs interfaces actives.

Interfaces actives

En entrée **Tout** **Rechercher** [Effacer le filtre](#)

Nombre maximum par page : **10**

5 routeur(s) sélectionné(s), 0 interface(s) sélectionnée(s) [Effacer la sélection](#)

Afficher : ☒ Tout ☐ Sélectionné

☐	Dernière interrogation	Adresse du routeur	Nom du routeur	Modèle	Interfaces	Composant de collecte
☒		10.0.40.33	US_NC_MNP_NOC_Router_External	Global par défaut	10	10.0.12.58
☒		10.0.40.34	10.0.40.34	Global par défaut	10	10.0.12.58
☒		10.0.42.1	cisco-2621-1	Global par défaut	10	10.0.12.58
☒		10.0.42.2	cisco-2621-2	Global par défaut	2	10.0.12.58
☒		10.0.42.3	cisco-2621-3	Global par défaut	2	10.0.12.58
☐		10.0.42.4	C3660B	Global par défaut	2	10.0.12.58
☐		10.0.42.5	Mimic2DevS11	Global par défaut	7	10.0.12.58
☐		10.0.42.6	Mimic2DevS12	Global par défaut	10	10.0.12.58
☐		10.0.42.7	Mimic2DevS13	Global par défaut	10	10.0.12.58
☐		10.0.42.8	Mimic2DevS14	Global par défaut	10	10.0.12.58

1 2 3 4 5

La page Interfaces actives inclut les options suivantes :

- Options de recherche : recherchez des routeurs, des interfaces ou des interfaces virtuelles personnalisées dont les adresses ou les noms correspondent à une chaîne de texte. Pour effacer la recherche, cliquez sur Effacer le filtre.
- Modifier : modifiez plusieurs attributs d'un routeur, d'une interface ou d'une interface virtuelle personnalisée.
- Fusionner : combinez les données de plusieurs interfaces physiques ou de plusieurs interfaces virtuelles personnalisées sélectionnées.
- Ajouter une interface virtuelle personnalisée : créez une interface virtuelle personnalisée à partir de l'interface physique sélectionnée.

Éléments de table de routeur

Les routeurs sont répertoriés dans la page Interfaces actives sous la forme de tables. Les tables de routeur contiennent les colonnes suivantes.

- Icône de flèche : cliquez sur cette icône pour développer la liste des interfaces pour le routeur.
- Case à cocher située dans la barre d'en-tête de colonne de la table Routeur : sélectionnez tous les routeurs ou effacez la sélection.
- Case à cocher située sur la ligne de routeur : sélectionnez un ou plusieurs routeurs pour effectuer l'une des actions suivantes :
 - Modifiez le nom, le profil SNMP, la version de profil SNMP, le port et le modèle d'application pour un seul routeur sélectionné.
 - Modifiez le profil SNMP, la version de profil SNMP, le port et le modèle d'application pour plusieurs routeurs sélectionnés.
 - Supprimez un ou plusieurs routeurs sélectionnés.

Les boutons Modifier et Supprimer sont désactivés si aucun routeur n'est sélectionné.

Colonnes de table

- Dernière interrogation : statut du routeur lors de la dernière interrogation.
 - Rouge : le routeur n'a pas été détecté.
 - Jaune : le routeur a été détecté, mais aucune donnée de flux n'a été reçue.
 - Vert : le routeur a été détecté et des données de flux ont été reçues.
- Adresse du routeur : adresse IP du routeur.
- Nom du routeur : nom du routeur affecté par l'utilisateur, tel que *routeur lab1*.
- Modèle : modèle associé à l'application.

- Interfaces : nombre total d'interfaces que le routeur contient.
- Composant de collecte : adresse IP du composant de collecte qui récupère les données à partir du routeur.

Éléments de table d'interface

Les interfaces et les interfaces virtuelles personnalisées sont répertoriées dans la page Interfaces actives, dans des tables imbriquées sous leurs routeurs parents. Pour afficher les interfaces d'un routeur, cliquez sur la flèche à côté du nom de routeur. Les tables d'interface contiennent les colonnes et les éléments suivants.

- Case à cocher située dans la barre d'en-tête de colonne de la table Interface : sélectionnez toutes les interfaces ou effacez la sélection.
- Case à cocher située sur la ligne d'interface : sélectionnez une ou plusieurs interfaces pour effectuer l'une des fonctions décrites dans la liste.
 - Modifiez le nom, la description, la vitesse d'entrée, la vitesse de sortie, le domaine et le type pour une seule interface sélectionnée.
 - Modifiez la vitesse d'entrée, la vitesse de sortie, le type et le domaine pour plusieurs interfaces sélectionnées. Vous pouvez sélectionner et modifier les interfaces à partir de plusieurs routeurs.
 - Supprimez une ou plusieurs interfaces sélectionnées. Vous pouvez sélectionner et supprimer les interfaces à partir de plusieurs routeurs.
 - Fusionnez une ou plusieurs interfaces sélectionnées.
 - Ajoutez une interface virtuelle personnalisée basée sur une interface physique.

Les boutons Modifier et Supprimer sont activés uniquement lorsqu'un ou plusieurs routeurs, interfaces ou interfaces virtuelles personnalisées sont sélectionnés.

Colonnes de table

- Statut du trafic : statut de l'interface lors de la dernière interrogation.
 - Rouge : interface inactive.
 - Vert : interface active.
- Classe : interface physique ou interface virtuelle personnalisée. L'icône d'interface physique est une zone grise contenant les lettres INT. L'icône d'interface virtuelle personnalisée affiche un V à côté de la zone.
- Nom de l'interface : nom de l'interface ou de l'interface virtuelle personnalisée affecté par l'utilisateur.
- Description : informations facultatives qu'un administrateur a ajoutées pour faciliter l'identification de l'interface ou de l'interface virtuelle personnalisée.
- Index : valeur d'index affectée à l'interface. La valeur Index pour une interface virtuelle personnalisée correspond à la valeur de l'interface parent.

- Type : type de connexion, tel que WAN, LAN ou VLAN.
- Vitesse en entrée : vitesse en entrée de l'interface ou de l'interface virtuelle personnalisée, si la vitesse est connue.
- Vitesse en sortie : vitesse en sortie de l'interface ou de l'interface virtuelle personnalisée, si la vitesse est connue.
- Domaine : domaine de l'interface, si plusieurs domaines ont été définis. Si l'environnement comprend un seul domaine, la colonne Domaine n'est pas affichée. Pour afficher l'association de client hébergé, sélectionnez la case à cocher située près de l'interface, puis cliquez sur Modifier.
- Remarques : lien vers les remarques de l'administrateur pour l'interface ou l'interface virtuelle personnalisée.

Recherche de routeur, d'interface ou d'interface virtuelle personnalisée

Utilisez la fonction de recherche de la page Interfaces actives pour localiser des routeurs, des interfaces ou des interfaces virtuelles personnalisées. Pour rechercher des cumuls, utilisez la fonction de recherche de la page Interfaces de cumul.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.
La page Interfaces actives s'ouvre et indique les routeurs actuels et leurs interfaces actives.
2. Introduisez une chaîne de texte dans le champ Rechercher. Recherchez des chaînes de texte entières ou partielles qui correspondent aux adresses, aux noms ou aux descriptions de routeurs, d'interfaces ou d'interfaces virtuelles personnalisées.

Remarque : N'utilisez pas de caractères génériques.

3. Cliquez sur Rechercher.
La liste est filtrée et uniquement les entrées correspondantes s'affichent. Si vous recherchez des interfaces ou des interfaces virtuelles personnalisées, la recherche renvoie une liste de routeurs qui contiennent les éléments correspondants. Lorsque vous développez les détails d'un routeur, tous les éléments s'affichent dans les sous-listes.

Pour effacer la recherche, cliquez sur Effacer le filtre.

Modification des détails d'un routeur, d'une interface ou d'une interface virtuelle personnalisée

Modifiez les propriétés d'un routeur, d'une interface ou d'une interface virtuelle personnalisée pour effectuer des corrections ou fournir des informations.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.
La page Interfaces actives s'ouvre et indique les routeurs actuels et leurs interfaces actives.
2. Recherchez les routeurs, les interfaces, ou les interfaces virtuelles personnalisées dont vous voulez modifier les détails. Pour afficher les interfaces d'un routeur, cliquez sur la flèche située près du nom de routeur.
3. Cochez la case à cocher située près des éléments à modifier. Vous pouvez modifier plusieurs interfaces et interfaces virtuelles personnalisées à la fois, ou modifier plusieurs routeurs à la fois. Toutefois, vous ne pouvez pas modifier un groupe de routeurs, interfaces et interfaces virtuelles personnalisées à la fois.
4. Cliquez sur Modifier.
La boîte de dialogue s'ouvre pour permettre la modification des éléments sélectionnés.
5. Modifiez les détails, si nécessaire.
 - Routeur (unique) : modifiez le nom, le domaine/client hébergé, le profil SNMP, la version de profil SNMP, le port et le modèle.
 - Routeur (plusieurs) : modifiez le nom, le domaine/client hébergé, le profil SNMP, la version de profil SNMP, la version de profil SNMP, le port et le modèle.

Les options de modification du profil SNMP, la version de profil SNMP et le port sont activées dès qu'une combinaison de domaine/client hébergé est sélectionnée.
 - Interface ou interfaces virtuelles personnalisées (unique) : modifiez le nom, la description, la vitesse d'entrée, la vitesse de sortie, le type de connexion et le domaine.
 - Interfaces ou interfaces virtuelles personnalisées (multiple) : modifiez la vitesse d'entrée, la vitesse de sortie, le type et le domaine.

- Interface virtuelle personnalisée (unique) : modifiez le nom d'interface, la description, la vitesse d'entrée, la vitesse de sortie, le type de connexion, le domaine et la liste des sous-réseaux.

Le paramètre domaine/client hébergé des interfaces et des interfaces virtuelles personnalisées ne doit pas nécessairement correspondre au paramètre du routeur parent.

6. Cliquez sur Enregistrer.

La boîte de dialogue Modifier le routeur ou Modifier l'interface se ferme. Les modifications sont reflétées dans la page Interfaces actives.

Suppression d'un routeur

Vous pouvez supprimer un routeur qui n'envoie plus de flux à CA Network Flow Analysis. Si vous supprimez un routeur, ses données d'historique, ses interfaces, ses interfaces virtuelles personnalisées et ses interruptions sont supprimées. La suppression affecte également tous les cumuls, les vues et les rapports qui incluent le routeur.

Procédez comme suit :

1. Vérifiez que le routeur n'envoie plus de flux à CA Network Flow Analysis.
2. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
3. Dans le menu de la page Administration, sélectionnez Interfaces : Physique et virtuelle.
La page Interfaces actives s'ouvre et affiche la liste des routeurs.
4. Cochez la case à côté du nom du routeur que vous voulez supprimer.
5. Cliquez sur Supprimer.
Un message s'ouvre vous invitant à confirmer la suppression.
6. Cliquez sur Oui.

Les résultats suivants se produisent :

- Le routeur est supprimé et le message de confirmation se ferme.
- Toutes les données d'historique associées sont purgées de façon permanente.
- Toutes les interfaces, les interfaces virtuelles personnalisées et les interruptions liées sont supprimées.
- Le routeur est supprimé de tous les cumuls associés.
- Les données des interfaces supprimées ne s'affichent plus dans les rapports personnalisés, ni dans les vues de la console NFA.

- Tous les rapports personnalisés définis pour afficher uniquement des interfaces à partir du routeur sont désactivés.
- Lorsque vous sélectionnez Activer les interfaces dans le menu Administration, le routeur est encore affiché dans la page Interfaces disponibles même s'il n'est plus répertorié dans la page Interfaces actives.

Personnalisation de la page Interfaces actives

Vous pouvez personnaliser l'apparence de la page Interfaces actives pour faciliter l'accès aux informations. Vous pouvez retrier les tables, afficher les détails des routeurs et modifier le nombre maximum d'interfaces et d'interfaces virtuelles personnalisées affichées dans les pages de détails sous chaque routeur.

Tri des données de table

Pour trier les données, cliquez sur un champ de menu. Par exemple, pour afficher tous les routeurs avec un indicateur de statut rouge, cliquez sur Dernière interrogation. Les résultats sont triés par l'horodatage Dernière interrogation.

Développement des détails pour les routeurs

Pour développer les détails d'un routeur, cliquez sur la flèche à gauche de la ligne du routeur. Une liste d'interfaces est affichée sous la ligne du routeur.

☐	Dernière interrogation	Adresse du routeur	Nom du routeur
☒		10.0.40.33	US_NC_MN_MNP_NOC,
Statut du trafic Classe Nom de l'interface			
☐			
☐		INT	G5/1
☐		INT	G5/2

Remarque : Le nombre de détails affichés dans la vue développée est limité par la valeur Nombre maximum par page définie pour le routeur sélectionné.

Pour afficher ou masquer les détails de tous les routeurs, les interfaces ou les interfaces virtuelles personnalisées, cliquez sur Tout développer ou Tout réduire dans le coin supérieur droit.

Modification du nombre de détails affichés

Pour modifier le nombre d'éléments affichés, sélectionnez une valeur maximum différente à partir de la liste déroulante Nombre maximum par page. Vous pouvez modifier la valeur du paramètre Nombre maximum par page pour la liste de routeurs. Vous pouvez également définir une valeur du paramètre Nombre maximum par page Max pour la sous-liste d'interfaces et d'interfaces virtuelles personnalisées sous chaque routeur.

En entrée **Tout** **Rechercher** [Effacer le filtre](#)

[Modifier](#)
[Supprimer](#)
[Fusionner](#)
[Ajouter une interface virtuelle personnalisée](#)

Nombre maximum par page : 10

0 routeur(s) sélectionné(s), 0 interface(s) sélectionnée(s) [Effacer la sélection](#)

Afficher : ☒ Tout ☐ Sélectionné [Tout développer](#) [Tout réduire](#)

☐	Dernière interrogation	Adresse du routeur	Nom du routeur	Modèle	Interfaces	Composant de collecte			
☒		10.0.40.33	US_NC_MN_MNP_NOC_Router_External	Global par défaut	10	10.0.12.58			
Nombre maximum par page : 10									
☐	Statut du trafic	Classe	Nom de l'interface	Description	Index de l'interface	Type	Vitesse en entrée	Vitesse de sortie	Remarques
☐		INT	Gi5/1	"External connection via MITnet/B24"	1	WAN MPI	1,00 Gbps	1,00 Gbps	
☐		INT	Gi5/2		2	Ethernet	1,00 Gbps	1,00 Gbps	

Utilisation des composants de collecte

Les administrateurs peuvent utiliser la page Composants de collecte de la console NFA pour afficher, ajouter, supprimer et modifier les détails des composants de collecte qui envoient les flux à la console NFA et à la console CA Performance Center.

Cette section comprend les rubriques suivantes :

[Ajout et suppression de Harvesters](#) (page 74)

[Modification des détails de composant de collecte](#) (page 75)

Ajout et suppression de Harvesters

Ajoutez et supprimez des Harvesters à partir de la page Harvester.

Pour ajouter un Harvester, effectuez les opérations de la rubrique [Ajout d'un Harvester](#) (page 26).

Pour supprimer un Harvester, effectuez les opérations décrites dans cette rubrique.

Remarque : Si vous supprimez un Harvester de CA Network Flow Analysis 9.1.3, vous ne pouvez plus ajouter la même instance de Harvester, sauf si le serveur d'installation est réimagé et le logiciel de Harvester est réinstallé. Une fois que vous avez supprimé un Harvester, vous ne pouvez plus récupérer les données déjà collectées.

Procédez comme suit :

1. Ouvrez la page Harvester.
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Système : Harvester.
La page Harvester s'ouvre et affiche un tableau contenant les informations sur les Harvesters connus.
2. Dans la ligne du Harvester que vous souhaitez supprimer, cliquez sur Supprimer.
Un message de confirmation s'affiche.
3. Cliquez sur Oui pour confirmer la suppression du Harvester.
Le Harvester est supprimé et n'est plus répertorié dans le tableau Harvester. La console NFA ne collecte plus les données des routeurs associés au Harvester supprimé. Les données de ces routeurs qui ont été collectées précédemment ne sont plus disponibles dans les rapports.

Modification des détails de composant de collecte

Modifiez les détails des composants de collecte à partir de la page Composant de collecte. Vous pouvez modifier l'adresse IP, la description et le paramètre client hébergé/domaine.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
2. Dans le menu de la page Administration, sélectionnez Système : Harvester.
La page Composant de collecte s'ouvre et affiche un tableau contenant les informations concernant les composants de collecte connus.
3. Sur la ligne Composant de collecte que vous souhaitez modifier, cliquez sur Modifier.
La boîte de dialogue Modifier le Harvester s'ouvre.
4. (Facultatif) Modifiez les paramètres suivants si nécessaire :

Adresse IP

Adresse IP du composant de collecte.

Description

(Facultatif) Informations supplémentaires pour faciliter l'identification du composant de collecte à partir de la page Composant de collecte.

Domaine

Client hébergé et domaine associés au Harvester

Toute modification apportée à ce paramètre affectera l'association de client hébergé/domaine de chaque routeur nouveau qui commence à exporter des données de flux et chaque nouvelle interface qui commence à générer des flux. Les routeurs et interfaces qui existent déjà conservent leurs associations client hébergé/domaine précédentes.

Le client hébergé affecte les profils SNMP disponibles pour l'interrogation de routeurs.

Le domaine affecte la disponibilité des routeurs et interfaces enfants à des opérateurs spécifiques.

Valeur par défaut : Client hébergé par défaut\Domaine par défaut.

Si aucun domaine IP personnalisé n'a été créé, la table Harvester inclut uniquement les colonnes Adresse IP et Description.

5. Lorsque vous avez apporté toutes les modifications nécessaires, cliquez sur Enregistrer.

Vos modifications sont enregistrées immédiatement et apparaissent dans le tableau Composant de collecte.

Chapitre 4: Personnalisation de CA Network Flow Analysis

Ce chapitre traite des sujets suivants :

[Introduction à la personnalisation](#) (page 77)
[Utilisation des groupes et des cumuls d'interface](#) (page 78)
[Définition des modèles pour les noms d'interfaces et les descriptions](#) (page 82)
[Création de groupes de protocoles](#) (page 86)
[Etiquetage de valeurs de type de service](#) (page 90)
[Création et gestion des groupes de types de services](#) (page 91)
[Personnalisation des noms de systèmes autonomes](#) (page 95)
[Nommage de routeurs](#) (page 98)
[Création de filtres de temps](#) (page 99)
[Création de périodes de génération de rapports](#) (page 101)

Introduction à la personnalisation

Vous pouvez personnaliser CA Network Flow Analysis pour permettre aux utilisateurs d'optimiser les résultats des rapports qu'ils affichent et génèrent.

Une fois que CA Network Flow Analysis est enregistré comme source de données auprès de CA Performance Center, vous devez effectuer plusieurs tâches de personnalisation et de configuration dans CA Performance Center. Vous utilisez CA Performance Center pour effectuer les tâches de configuration des utilisateurs, des rôles, des profils SNMP et de plusieurs types de groupes.

En tant qu'administrateur de CA Network Flow Analysis, vous pouvez effectuer les tâches de personnalisation suivantes dans la console NFA :

- Création et gestion des cumuls d'interface
- Création et gestion des modèles d'interface
- Création de groupes de protocoles
- Etiquetage de valeurs de type de service
- Création de groupes de types de service
- Nommage de routeurs
- Création de filtres de temps
- Création de périodes de génération de rapports

Utilisation des groupes et des cumuls d'interface

Vous pouvez créer et gérer des groupes d'interface dans CA Performance Center, une fois que CA Network Flow Analysis y est enregistrée comme source de données. Les groupes d'interfaces personnalisés permettent aux utilisateurs d'optimiser les résultats des rapports et des analyses personnalisés. Par exemple, vous pouvez permettre aux utilisateurs de configurer des rapports personnalisés pour des groupes d'interface selon l'emplacement géographique, la vitesse d'interface, les sites T1 ou l'équilibrage de la charge.

Vous pouvez créer et gérer des cumuls d'interface à partir de la console NFA. Un cumul d'interface associe le trafic provenant de plusieurs interfaces de telle façon que les rapports sont générés pour un trafic unifié. Par exemple, supposez que vous avez deux circuits dont la charge est équilibrée et que vous voulez générer un rapport sur les interfaces comme s'il s'agissait d'une unité unique. Les cumuls vous permettent de générer des rapports sur les interfaces en une unité unique, sans pour autant devoir recourir à la création de rapport personnalisé à cet effet. Tous les cumuls s'affichent dans l'index d'interface sous l'étiquette *Cumuls*.

Remarque : Vous pouvez cumuler des interfaces uniquement lorsque leurs données sont collectées par le même composant de collecte. Ne cumulez aucune interface à partir de plusieurs composants de collecte.

Création de cumuls d'interface

Créer des cumuls d'interface pour associer le trafic provenant de plusieurs interfaces de telle façon que les rapports sont générés pour un trafic unifié.

Par exemple, vous créez des cumuls pour chaque région géographique. Les opérateurs utilisent les cumuls dans des rapports pour vérifier et comparer les totaux de ces régions. Avant la création de cumuls, les opérateurs rencontraient les problèmes suivants :

- Les données étaient clairessemées sur plusieurs rapports.
- Les valeurs n'étaient pas cumulées par région ; les synthèses et les comparaisons rapides étaient donc difficiles à effectuer.
- Les opérateurs passaient trop longtemps à concevoir des rapports spécialisés pour la collecte de données et la création des totaux requis.

Procédez comme suit :

1. Affichez la page Interfaces de cumul :

- a. Dans le menu de console NFA, sélectionnez Administration.

La page Administration s'ouvre.

- b. Dans le menu de la page Administration, sélectionnez Interfaces : Cumuls.

La page Interfaces de cumul s'ouvre et affiche la liste des cumuls d'interface actuels.

2. Cliquez sur Nouveau.

La page est actualisée pour afficher les options permettant l'ajout d'un cumul.

Sélectionnez les interfaces à ajouter au cumul à l'aide de l'une des méthodes suivantes :

- *Sélection de routeurs* : cochez les cases à côté d'un ou de plusieurs noms de routeur. Vous pouvez sélectionner un ou plusieurs routeurs, ou une combinaison de routeurs et d'interfaces individuelles pour un routeur qui n'est pas sélectionné. Lorsqu'un routeur a été sélectionné, aucune de ses interfaces individuelles ne peut être sélectionnée.
- *Sélection d'interfaces* : cliquez sur Tout développer ou cliquez sur la flèche à côté d'un nom de routeur, puis sélectionnez les interfaces dans la liste. Pour sélectionner toutes les interfaces d'un routeur, cochez la case de la ligne de titre.
- *Filtrage de la liste pour rechercher des routeurs ou des interfaces* : pour filtrer l'affichage, saisissez une chaîne de texte dans la zone de recherche, puis cliquez sur Rechercher. Vous pouvez rechercher un nom complet, un nom partiel, l'adresse d'un routeur ou l'adresse d'une interface. La liste des routeurs/interfaces est filtrée pour afficher les routeurs correspondants ou les routeurs qui contiennent des interfaces correspondantes.

- *Filtrage de la liste pour vérifier les sélections* : cliquez sur Afficher la sélection pour appliquer un filtre et afficher uniquement les routeurs sélectionnés ou qui contiennent des interfaces sélectionnées. Vous pouvez associer cette fonction à une chaîne de recherche et utiliser l'option Tout développer pour localiser et vérifier rapidement vos sélections.

3. Spécifiez les valeurs suivantes, puis cliquez sur Enregistrer :

- Routeurs et/ou Interfaces : sélectionnez un ou plusieurs routeurs ou interfaces répertoriés au bas de la page. Vos sélections sont ajoutées au cumul.
- Nom du cumul : spécifiez un nom pour le cumul.
- Description (facultatif) : ajoutez une note pour faciliter l'identification du cumul.
- Vitesse d'entrée (facultatif) : spécifiez la vitesse d'entrée des interfaces sélectionnées.
- Vitesse de sortie (facultatif) : spécifiez la vitesse de sortie des interfaces sélectionnées.

Si vous ne spécifiez aucune vitesse d'entrée et de sortie, les valeurs sont définies sur 0 par défaut. Les vitesses inexacts rendent certains résultats de rapport inexacts, notamment le pourcentage d'utilisation.

- Type (facultatif) : sélectionnez le mode de connexion de l'interface dans la liste Type, comme WAN ou Ethernet.

Si vous ne spécifiez aucun type d'interface, le type est défini sur Inconnu par défaut.

Le cumul est automatiquement déployé en quelques minutes.

Modification d'un cumul d'interface

Modifiez un cumul d'interface pour sélectionner différentes interfaces à cumuler ou pour modifier le nom du cumul, la description, la vitesse ou le type d'interface.

Procédez comme suit :

1. Affichez la page Interfaces de cumul :

- a. Dans le menu de console NFA, sélectionnez Administration.

La page Administration s'ouvre.

- b. Dans le menu de la page Administration, sélectionnez Interfaces : Cumuls.

La page Interfaces de cumul s'ouvre et affiche la liste des cumuls d'interface actuels.

2. Cochez la case à côté du cumul que vous voulez modifier, puis cliquez sur Modifier.
La page passe en mode Modifier un cumul et les options de modification sont disponibles.
3. Apportez les modifications nécessaires : ajoutez ou supprimez des interfaces, ou modifiez le nom du cumul, la description, la vitesse d'entrée/de sortie ou le type.
4. Cliquez sur Enregistrer.
Vos modifications sont enregistrées et vous revenez à la liste des cumuls.

Modification de plusieurs cumuls d'interface

Modifiez plusieurs cumuls d'interface pour changer rapidement la vitesse d'interface ou le type d'interface.

Procédez comme suit :

1. Affichez la page Interfaces de cumul :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Interfaces : Cumuls.
La page Interfaces de cumul s'ouvre et affiche la liste des cumuls d'interface actuels.
2. Cochez la case à côté du cumul que vous voulez modifier. Pour sélectionner tous les cumuls, cochez la case de la ligne de titre.
3. Cliquez sur Modifier.
La boîte de dialogue Modifier les interfaces s'ouvre.
4. Modifier les paramètres suivants si nécessaire :
 - Vitesse d'entrée (facultatif) : vitesse d'entrée des interfaces sélectionnées.
 - Vitesse de sortie (facultatif) : vitesse de sortie des interfaces sélectionnées.
 - Type (facultatif) : mode de connexion de l'interface, comme WAN ou Ethernet.
5. Cliquez sur Enregistrer.
Vos modifications sont enregistrées et vous revenez à la liste des cumuls.

Suppression de cumuls d'interface

Supprimez les cumuls d'interface dont vous n'avez plus besoin.

Procédez comme suit :

1. Affichez la page Interfaces de cumul :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Interfaces : Cumuls.
La page Interfaces de cumul s'ouvre et affiche la liste des cumuls d'interface actuels.
2. Cochez la case située à côté de chaque cumul à supprimer.
3. Cliquez sur Supprimer.
4. Dans le message de confirmation qui s'affiche, cliquez sur Oui.
Tous les cumuls sélectionnés sont supprimés automatiquement.

Définition des modèles pour les noms d'interfaces et les descriptions

Modifiez les règles qui déterminent l'affichage des noms et des descriptions d'interface dans la console NFA à l'aide d'une des procédures suivantes :

- Créez un modèle d'interface et définissez-le en tant que modèle actif pour CA Network Flow Analysis.
- Modifiez le modèle d'interface actuel.
- Affinez l'attribution des noms d'interfaces pour des vues de console NFA spécifiques à l'aide de la page Paramètres de l'application.

Vous pouvez créer plusieurs modèles d'interface, mais seul le modèle d'interface actuellement sélectionné déterminera les noms et les descriptions d'interfaces dans la console NFA, dans ses vues et dans ses rapports imprimés.

Le modèle d'interface actuellement sélectionné affecte également les noms d'interface et les descriptions dans certaines vues CA Performance Center des données CA Network Flow Analysis. Les emplacements suivants dans CA Performance Center peuvent afficher des noms et des descriptions d'interface différents : pages d'interface (onglet Détails), pages d'inventaire et vues de tendance. Pour personnaliser les descriptions d'interface dans CA Performance Center, appliquez des substitutions de descriptions d'interface à des domaines spécifiques. Ces substitutions sont décrites dans la rubrique Ajout d'un domaine IP dans l'aide de CA Performance Center ainsi que dans le fichier Readme de CA Network Flow Analysis 9.1.2.

Création d'un modèle d'interface personnalisé

Créez un modèle d'interface personnalisé pour modifier l'affichage des noms d'interface et des descriptions dans la console NFA. En créant un modèle d'interface sans modifier le modèle actuel, vous pouvez l'adapter aux différents formats.

Procédez comme suit :

1. Affichez la page Modèles d'interface dans la console NFA :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Système : Modèles.
La page Modèles d'interface s'ouvre.

2. Cliquez sur Ajouter.

La page Modèles d'interface affiche les options d'ajout de modèle d'interface.

3. Spécifiez les paramètres de modèle d'interface :
 - Nom : nom affiché dans la liste de modèles.
 - Nom d'interface : propriétés, texte ou propriétés et texte qui constituent le nom de chaque interface dans la console NFA.
 - Description de l'interface : propriétés, texte ou propriétés et texte qui constituent la description de chaque interface dans la console NFA.

Utilisez les propriétés de la liste suivante pour les deux paramètres :

- *[Alias de l'unité]* : nom d'unité (routeur) affiché dans la console NFA.
- *[Nom de l'unité]* : nom DNS ou adresse IP de l'unité (routeur).
- *[ifDescr]* : description de l'interface provenant de la valeur ifDescr d'origine dans la table ifEntry SNMP (sauf si la description d'interface a été personnalisée). Si la description d'interface a été personnalisée sur la page Interfaces actives, la valeur personnalisée est utilisée.
- *[ifAlias]* : alias de l'interface
- *[ifName]* : nom de l'interface provenant de la valeur ifName d'origine dans la table ifEntry SNMP (sauf si le nom d'interface a été personnalisé). Si le nom de l'interface a été personnalisé sur la page Interfaces actives, la valeur personnalisée est utilisée.
- *[Nom du port]* : nom du port, qui peut être le numéro de port.
- *[ifIndex]* : identificateur numérique unique pour l'interface tel que défini dans la table ifEntry SNMP
- *[ifType]* : type d'interface, tel que défini dans le champ ifType de la table SNMP ifEntry.

4. Cliquez sur Soumettre.

Le nouveau modèle est créé et ajouté à la liste de modèles. Les options supplémentaires sont supprimées de la page Modèles d'interface.

5. (Facultatif) Appliquez le modèle : sélectionnez le modèle dans la liste au haut de la page Modèles d'interface.

Le modèle est appliqué à la console NFA presque immédiatement. Les vues CA Performance Center qui utilisent le modèle affichent les modifications lors de la prochaine synchronisation, qui a automatiquement lieu dans un délai de 5 minutes.

6. (Facultatif) Réviser le modèle modifié. Par exemple, réviser les nouvelles étiquettes sur les pages Interface et Présentation de l'entreprise.

Conventions des modèles d'interface

Les paramètres de modèle d'interface comprennent des propriétés, du texte brut ou des propriétés et du texte brut. Les conventions suivantes s'appliquent aux modèles d'interface :

- Entourez les propriétés de crochets.
- Séparez les différentes propriétés d'une barre verticale. La première propriété qui renvoie une valeur est affichée. Spécifiez autant de propriétés que nécessaires pour toutes les interfaces dont les propriétés sont définies de manière incomplète.
- Pour afficher les noms d'interface ou les descriptions en texte brut, incluez le texte sans utiliser de parenthèses.

Modification d'un modèle d'interface

Modifiez un modèle d'interface pour modifier l'affichage des noms d'interface et des descriptions dans la console NFA lorsque le modèle est sélectionné.

Procédez comme suit :

1. Affichez la page Modèles d'interface dans la console NFA :

- a. Dans le menu de console NFA, sélectionnez Administration.

La page Administration s'ouvre.

- b. Dans le menu de la page Administration, sélectionnez Système : Modèles.

La page Modèles d'interface s'ouvre.

2. Sélectionnez le modèle dans la liste en haut de la page.

3. Cliquez sur Modifier.

Un message de confirmation s'ouvre pour vous prévenir des conséquences de la modification du modèle actuel.

4. Cliquez sur OK dans le message de confirmation.

Le contenu des champs Nom de l'interface et Description de l'interface devient modifiable dans la page Modèles d'interface.

5. Spécifiez les paramètres de modèle d'interface :

- Nom de l'interface : texte et/ou propriétés qui constituent le nom de chaque interface dans l'interface utilisateur de CA Network Flow Analysis.
- Description de l'interface : texte et/ou propriétés qui apparaissent dans la description de chaque interface dans l'interface utilisateur de CA Network Flow Analysis.

Définissez les deux paramètres avec les propriétés de la liste dans la rubrique sur la [création d'un modèle](#) (page 83):

6. Cliquez sur Mettre à jour.

Le contenu des champs Nom de l'interface et Description de l'interface n'est plus modifiable.

Les noms d'interface et les définitions sont affichés dans la console NFA presque immédiatement. Les vues CA Performance Center qui utilisent le modèle affichent les modifications lors de la prochaine synchronisation, qui a automatiquement lieu dans un délai de 5 minutes.

7. (Facultatif) Révisez le modèle modifié. Par exemple, révisez les nouvelles étiquettes sur les pages Interface et Présentation de l'entreprise.

Modification du paramètre de l'application pour les noms d'interface

Pour changer la convention d'attribution des noms des interfaces, vous pouvez utiliser un paramètre de la page Paramètres de l'application. Le paramètre par défaut ajoute le nom de l'unité avant le nom de l'interface. Ce paramètre affecte la manière dont les noms d'interface s'affichent dans certaines vues de rapport de console NFA, telles que les vues de présentation de l'entreprise, les pages d'interfaces et les récapitulatifs d'interfaces des rapports personnalisés.

Les noms d'interface obtenus peuvent inclure des doublons superflus. Par exemple, si une unité et une interface sont toutes les deux nommées Device1, le nom d'interface Device1::Device1 est affiché par défaut. L'exemple suivant illustre cette répétition.

Statut	Interface
■	rtr-5.25-austin.netqos.com::AnotherATM
■	rtr-5.25-austin.netqos.com::AnotherATM

Pour éliminer cette duplication, dans la page Paramètres de l'application, modifiez le paramètre Afficher le nom de l'unité.

Procédez comme suit :

1. Affichez la page Paramètres de l'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Système : Paramètres de l'application.
La page Paramètres de l'application s'affiche.
2. Définissez la valeur de l'option Afficher le nom de l'unité sur False.
3. Cliquez sur Enregistrer.
Lorsque la valeur de Afficher le nom de l'unité est False, les noms des unités dans les rapports et les vues ne sont pas ajoutés aux noms d'interfaces.

Création de groupes de protocoles

Les groupes de protocoles agissent comme des filtres pour les données de rapport. L'administrateur peut configurer des groupes de protocoles personnalisés contenant des protocoles pour des types particuliers de trafic réseau.

Par exemple, si les opérateurs veulent créer des rapport sur le trafic réseau pour différents types d'applications, telles que la messagerie, la vidéoconférence, la voix sur IP et les médias de diffusion en continu. Aucun groupe de protocoles par défaut n'est défini à cette fin : l'administrateur crée donc un groupe de protocoles personnalisé pour chaque type d'application. Chaque groupe de protocoles inclut toutes les valeurs de protocole qui sont utilisées dans l'entreprise pour les applications cibles.

Les opérateurs peuvent filtrer des données de rapport à l'aide des groupes de protocoles par défaut maintenus par CA Network Flow Analysis automatiquement et des groupes de protocoles personnalisés. Lorsqu'un groupe de protocoles est utilisé comme un filtre, les opérateurs n'ont pas besoin d'ajouter de filtres pour chaque protocole.

Remarque : Dans un environnement multi-domaine, le contenu de groupes de protocoles affiche tous les groupes de noms de protocoles personnalisés spécifiques de domaines que les administrateurs ont créés.

Les rubriques suivantes indiquent aux administrateurs de CA Network Flow Analysis comment créer un groupe de protocoles de shell, configurer le groupe de protocoles, et ensuite réviser et modifier les paramètres du groupe de protocoles.

Création d'un groupe de protocoles de shell

Créez des groupes de protocoles pour aider les opérateurs à obtenir rapidement des résultats optimaux à partir des rapports d'analyse et personnalisés.

Procédez comme suit :

1. Ouvrez la page Configuration du groupe de protocoles :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Groupes : Groupes de protocoles.
La page Configuration du groupe de protocoles s'ouvre et affiche des informations sur le groupe de protocoles actuellement sélectionné.
2. Cliquez sur Ajouter.
Les options permettant d'identifier un nouveau groupe de protocoles apparaissent dans la page Configuration du groupe de protocoles.
3. Entrez les valeurs dans les zones Nom du groupe et Description.
Le nom et la description s'affichent aux emplacements suivants dans CA Network Flow Analysis :
 - Liste des groupes de protocoles sur la page Configuration du groupe de protocoles
 - Index des groupes de protocoles qu'un opérateur peut afficher dans l'assistant de création de rapports pour définir un rapport d'analyse ou personnaliséUn nouveau groupe de protocoles de shell est créé. Le nouveau nom de groupes de protocoles est ajouté à la liste des groupes de protocoles sur la page Configuration du groupe de protocoles.
Vous pouvez configurer le groupe de protocoles de shell.

Configuration du groupe de protocoles

Après la création d'un groupe de protocoles de shell, l'étape suivante consiste à configurer le groupe de protocoles.

Procédez comme suit :

1. Dans la page Configuration du groupe de protocoles, sélectionnez le groupe de protocoles dans la liste Groupe de protocoles.
2. Cliquez sur Liste.
Les options de configuration sont ajoutées à la page Configuration du groupe de protocoles.

3. (Facultatif) Réviser et corriger le paramètre Domaine si nécessaire.

Remarque : Le paramètre Domaine est affiché uniquement lorsqu'un environnement contient plusieurs domaines.

Le contenu du groupe de protocoles sélectionné affiche les noms des protocoles du domaine sélectionné. Si un administrateur a défini des noms propres au domaine pour les protocoles, la sélection de ce domaine affichera les noms de protocole correspondants.

Le paramètre Domaine ne limite pas l'accès au groupe de protocoles ou aux rapports qui utilisent le groupe de protocoles comme filtre.

4. Sélectionnez les protocoles pour le groupe :

- a. Cliquez sur Ajouter/supprimer.

Une boîte de dialogue s'ouvre. Elle contient la liste des protocoles disponibles et une liste des protocoles actuellement inclus dans la liste.

Si le lien Ajouter/Supprimer n'est pas visible, cliquez sur Liste.

- b. Dans le volet supérieur, sélectionnez les protocoles que vous voulez ajouter au groupe.

Pour sélectionner plusieurs protocoles à ajouter simultanément, utilisez les touches Majuscule et Contrôle.

Pour filtrer la liste de protocoles, saisissez une chaîne de recherche dans le champ Filtrer la liste de protocoles, puis cliquez sur Appliquer. Par exemple, pour afficher uniquement les protocoles UDP, entrez **udp**.

- c. Cliquez sur Ajouter.

Les protocoles sélectionnés sont ajoutés à la liste de protocoles.

- d. Dans le volet inférieur, sélectionnez les protocoles que vous voulez supprimer du groupe.

- e. Cliquez sur Supprimer.

Les protocoles sélectionnés sont supprimés de la liste de protocoles.

- f. Cliquez sur Terminé lorsque vous avez terminé de configurer le contenu du groupe de protocoles.

Pour réviser une liste de groupes de protocoles contenant un protocole particulier, sélectionnez le protocole et cliquez sur Accéder au protocole. La page Configuration du protocole s'ouvre et affiche la liste de protocoles contenant le protocole sélectionné.

Le groupe de protocoles est configuré selon vos paramètres. Les opérateurs peuvent sélectionner le groupe de protocoles configuré comme filtre pour un rapport d'analyse ou personnalisé.

Remarque : Les opérateurs peuvent définir des rapports uniquement si leurs paramètres d'utilisateur le permettent.

Révision des paramètres de groupe de protocoles

Une fois le groupe de protocoles créé et après l'exécution des rapports par les opérateurs utilisant le groupe de protocoles comme filtre, vous pouvez apporter des modifications. Vous pouvez renommer le groupe de protocoles et utiliser un nom décrivant l'utilisation que les opérateurs feront de ce groupe. Vous pouvez également changer la liste de protocoles inclus dans le groupe.

Procédez comme suit :

1. Dans la page Configuration du groupe de protocoles, sélectionnez le groupe de protocoles dans la liste Groupe de protocoles.
2. (Facultatif) Modifiez le nom ou la description du groupe de protocoles :
 - a. Cliquez sur Modifier.
La page Modifier un groupe de protocoles s'ouvre.
 - b. Changez les valeurs des champs Nom du groupe et Description pour décrire clairement l'objectif du groupe de protocoles.
 - c. Cliquez sur Soumettre.
Le nom et la description sont mis à jour dans la liste de la page Configuration du groupe de protocoles et dans la page Index des groupes de protocoles.

3. (Facultatif) Réviser la liste de protocoles inclus :

- a. Cliquez sur Liste.
Une table répertoriant les protocoles est ajoutée au bas de la page.
- b. Sélectionnez le domaine approprié dans la liste de domaines (si les noms de protocoles personnalisés ont été définis).

Remarque : Le paramètre Domaine est affiché uniquement lorsque plusieurs domaines sont configurés pour un environnement.

Pour plus d'informations sur le paramètre Domaine, consultez l'étape 3 dans la section [Configuration du groupe de protocoles](#) (page 87).

- c. Cliquez sur Ajouter/Supprimer et modifiez le contenu du groupe de protocoles si nécessaire
Pour plus d'informations sur cette étape, consultez l'étape 4 dans la section [Configuration du groupe de protocoles](#) (page 87).
- d. Cliquez sur Terminé lorsque vous avez terminé de configurer le contenu du groupe de protocoles.

Le groupe de protocoles est configuré selon vos paramètres. Les opérateurs peuvent sélectionner le groupe de protocoles reconfiguré comme filtre pour un rapport d'analyse ou personnalisé.

Etiquetage de valeurs de type de service

Vous pouvez créer des étiquettes, ou des descriptions, pour les valeurs de type de service afin de vous assurer que les opérateurs connaissent le service associé aux différentes valeurs de type de service. Si vous n'étiquetez aucune valeur de type de service, la valeur de type de service numérique est affichée par défaut.

Remarque : Les étiquettes de type de service que vous créez concernent toutes les utilisations du type de service dans le domaine affecté, mais ne concernent pas les étiquettes de type de service d'autres domaines.

Procédez comme suit :

1. La page Configuration du type de service s'affiche.
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Noms de type de service.
La page Configuration du type de service s'ouvre et affiche des informations sur le type de service et le domaine sélectionnés.
2. Environnement de domaine multiple uniquement : sélectionnez le domaine qui contient les valeurs de type de service que vous voulez modifier.
3. Sélectionnez une valeur de type de service dans la liste, puis cliquez sur Modifier.
La description peut être modifiée.
4. Saisissez une nouvelle description pour la valeur de type de service dans la zone de description et cliquez sur Enregistrer.
La modification est enregistrée et les champs Description et Valeur pour le type de service sélectionné sont mis à jour.

Remarque : Vous pouvez également utiliser la page Configuration du type de service pour ajouter des valeurs de type de service à des groupes de types de service ou les supprimer. Sélectionnez le client hébergé/domaine et la valeur de type de service, puis cliquez sur le lien Ajouter/supprimer dans la partie supérieure de la liste des groupes de types de service. La boîte de dialogue Index de groupe de types de service s'ouvre. Apportez les modifications nécessaires aux groupes configurés par les utilisateurs. Vous ne pouvez pas modifier les groupes de types de service prédéfinis.

Création et gestion des groupes de types de services

Un administrateur peut créer des groupes de types de services qui agissent comme des filtres pour les données de rapport. L'administrateur configure chaque groupe de types de service pour contenir les valeurs de types de service qui caractérisent un type particulier de trafic réseau. Les opérateurs peuvent utiliser le groupe de types de service comme filtre dans des rapports au lieu d'ajouter des filtres pour chaque valeur de types de service.

Par exemple, si les opérateurs veulent générer des rapports sur le trafic réseau pour le groupe Low Drop Assured Forwarding (acheminement assuré à faible taux d'abandon). Ce groupe est un groupe de valeurs de types de services affectées à des applications prioritaires par rapport au trafic moins critique. L'administrateur crée un groupe de types de services nommé Low drop (faible taux d'abandon), qui inclut toutes les valeurs de types de services pour AF11, AF21, AF31 et AF41. Les opérateurs peuvent créer un rapport sur le trafic des applications à l'aide du nouveau groupe Low Drop ToS (types de services de faible taux d'abandon).

Remarque : Les groupes de types de services sont disponibles dans tous les domaines en tant que filtres pour les rapports d'analyse et les rapports personnalisés. Les étiquettes de types de service affichées pour le contenu d'un groupe de types de service sont propres à un domaine.

Création d'un groupe de types de services de shell

Créez des groupes de types de services pour permettre aux utilisateurs d'obtenir rapidement des résultats optimaux à partir des rapports d'analyse et personnalisés.

Procédez comme suit :

1. Ouvrez la page Configuration du groupe de types de services :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Groupes : Groupes de types de service.
La page Configuration du groupe de types de services s'ouvre et affiche des informations sur le groupe de types de services et le domaine sélectionnés.
2. Cliquez sur Ajouter.
Les options de cette page permettent d'identifier un nouveau groupe de types de services de shell.

3. Entrez les valeurs dans les zones Nom et Description.

Le nom et la description s'affichent aux emplacements suivants :

- Liste des groupes de types de services sur la page Configuration du groupe de types de services
- Index des groupes de types de services qu'un utilisateur peut afficher dans l'assistant de création de rapports pour définir un rapport d'analyse ou personnalisé

4. Cliquez sur Ajouter.

Un nouveau groupe de types de services de shell est créé. Le nouveau nom du groupe de types de services s'affiche dans la liste de groupes de types de services sur la page Configuration du groupe de types de services.

Vous pouvez ajouter des valeurs au groupe de types de services de shell.

Ajout de valeurs de types de services au groupe

Après la création d'un groupe de types de services de shell, l'étape suivante consiste à ajouter des valeurs au groupe.

Procédez comme suit :

1. Dans la page Configuration du groupe de types de services, sélectionnez le groupe de types de services dans la liste Groupe de types de services.
2. (Facultatif) Sélectionnez une combinaison client hébergé/domaine dans la Liste des domaines, dans le cas où plusieurs domaines existent et que vous avez créé plusieurs étiquettes de type de service spécifiques aux domaines.

Si un seul domaine existe, aucun paramètre Domaine n'est affiché.

Sélectionnez une combinaison client hébergé/domaine pour afficher les étiquettes de types de service disponibles et spécifiques au domaine et identifier facilement les valeurs de type de service à utiliser. Le groupe de types de services ne sera pas restreint au domaine sélectionné : les groupes sont disponibles dans tous les domaines.

3. Cliquez sur Ajouter/supprimer.

La boîte de dialogue Index des types de service s'affiche. La liste des types de services affiche les valeurs d'index de types de services et les étiquettes de types de services définies pour le domaine actuellement sélectionné.

4. Sélectionnez les valeurs de types de services que vous voulez ajouter en cliquant sur les cases à cocher correspondantes.

5. Faites défiler la liste vers le bas et cliquez sur Enregistrer.

Les valeurs sont ajoutées au groupe de types de services.

Un opérateur peut sélectionner le groupe dans l'index de groupes de types de services lors de la définition d'un rapport d'analyse ou personnalisé.

Remarque : Pour définir des rapports, l'opérateur doit disposer du rôle et des paramètres de groupe d'autorisations nécessaires.

Modification du contenu des groupes de types de service

Vous pouvez modifier la liste des valeurs de type de service incluses dans un groupe de types de service afin d'apporter des corrections ou de changer le but du groupe.

Les groupes de types de service sont indépendants des domaines ; les valeurs de type de service incluses dans un groupe de types de service restent inchangées lorsque vous basculez vers un domaine différent.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.

La page Administration s'ouvre.

2. Dans le menu de la page Administration, sélectionnez Groupes : Groupes de types de service.

La page Configuration du groupe de types de service s'ouvre et contient des informations sur le groupe de types de service et la combinaison client hébergé/domaine sélectionnés.

3. Sélectionnez le groupe de types de service à modifier dans la liste Sélectionner un groupe de types de service.

La page Configuration du groupe de types de service s'ouvre et affiche des informations sur le groupe de types de service et le domaine sélectionnés.

Remarque : Vous ne pouvez pas modifier les groupes prédéfinis, comme le groupe Tous les types de service dans le domaine par défaut.

4. (Environnements à multiples domaines uniquement) Sélectionnez une combinaison client hébergé/domaine dans la liste Domaine, dans le cas où plusieurs domaines existent et qu'un administrateur a créé des étiquettes de type de service. Les étiquettes de type de service sont propres au domaine.

Le paramètre Domaine est affiché uniquement lorsque plusieurs domaines existent.

5. Cliquez sur le lien Ajouter/supprimer situé au-dessus de la liste de valeurs de type de service incluses dans le groupe.

La boîte de dialogue Index des types de service s'affiche. La liste des types de service affiche les étiquettes de type de service définies pour le domaine actuellement sélectionné.

6. Cochez les cases ou désélectionnez-les pour inclure uniquement les valeurs de type de service que vous souhaitez.
7. Lorsque vous avez effectué vos modifications, cliquez sur Enregistrer. La liste des valeurs de type de service est mise à jour.

Suppression de groupes de types de service

Vous pouvez supprimer les groupes de types de service dont vous n'avez plus besoin. Une fois que vous les avez supprimés, ils ne sont plus répertoriés dans la liste des groupes de types de service.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
2. Dans le menu de la page Administration, sélectionnez Groupes : Groupes de types de service.
La page Configuration du groupe de types de service s'ouvre et affiche des informations sur le groupe de types de service et le domaine sélectionnés.
3. Sélectionnez le groupe de types de service à supprimer dans la liste Sélectionner un groupe de types de service.
Sélectionnez un groupe de types de service configurable. Par exemple, vous ne pouvez pas modifier le groupe Tous les types de service.
Remarque : Le paramètre Domaine, s'il existe, n'a aucun effet sur la liste des groupes de types de service disponibles. Si vous supprimez un groupe de types de service, il est supprimé pour tous les domaines.
4. Cliquez sur Supprimer.
Un message de confirmation s'affiche.
5. Cliquez sur OK.
Le groupe sélectionné est supprimé. La liste des valeurs de type de service est mise à jour.

Personnalisation des noms de systèmes autonomes

Les rapports d'interface dans CA Network Flow Analysis contenant des données relatives au trafic du système autonome (AS) répertorient généralement ces systèmes par nom et numéro. Les administrateurs peuvent personnaliser les noms de systèmes autonomes qui apparaîtront dans les rapports pour utiliser des noms plus courts ou descriptifs.

Par exemple, si les opérateurs consultent fréquemment des rapports sur le trafic réseau tel qu'AS 4000000. L'étiquette portant le nom du système autonome par défaut est UUNET-CANADA - Progressive Communications Services, Inc. d/b/a Acme Business (4000000). L'administrateur peut personnaliser le nom du système autonome pour afficher le nom suivant dans le rapport : Acme (4000000).

Les noms de systèmes par défaut sont spécifiques du domaine. Les noms qui s'affichent dans les rapports proviennent du domaine de l'interface pour le rapport.

Les rubriques de cette section décrivent la procédure de révision et de modification des noms de systèmes autonomes.

Pour effectuer ces tâches, configurez le flux NetFlow ou le flux compatible avec NetFlow pour la prise en charge de la génération de rapports pour des systèmes autonomes. Pour afficher des données de systèmes autonomes pertinentes dans les rapports, vous devez activer cette prise en charge, car NetFlow n'exporte pas des informations de systèmes autonomes complètes par défaut. Pour plus d'informations sur l'activation des données de systèmes autonomes, consultez l'article de la base de connaissances TEC562036, Viewing AS Numbers in Reports, sur le site de CA Support (<http://ca.com/support>).

Les données de systèmes autonomes affichent la valeur Système autonome 0 dans les rapports dans les cas suivants :

- Le flux n'est pas configuré pour prendre en charge la génération de rapports pour des systèmes autonomes.
- Le routage de la source des données est inconnu.
- Les données proviennent du système local.

Révision des noms de systèmes autonomes

Réviser les références des systèmes autonomes dans les rapports d'interfaces pour votre entreprise et localiser les numéros de systèmes autonomes en cours d'utilisation qui contiennent des références de systèmes autonomes longs et peu clairs.

Rapports d'interfaces qui contiennent des références de systèmes autonomes :

- Table du récapitulatif des tronçons suivants du système autonome (interface unique)
- Graphiques à secteurs, graphiques de tendance et tables de récapitulatif des N principaux systèmes autonomes

Procédez comme suit :

1. Collectez des informations concernant les noms de systèmes autonomes utilisés dans les rapports d'interface pour votre entreprise.

La liste de tous les numéros et noms de systèmes autonomes est grande. Vous ne personnaliserez pas tous les noms de systèmes autonomes de la liste.

Par exemple, créez la liste des noms de systèmes autonomes souvent utilisés en examinant les rapports des systèmes autonomes ou en demandant aux opérateurs quels systèmes autonomes ils suivent.

2. Affichez la page Noms des systèmes autonomes :

- a. Dans le menu de console NFA, sélectionnez Administration.

La page Administration s'ouvre.

- b. Sélectionnez la page Définir une application : Noms des systèmes autonomes dans le menu de la page Administration.

La page Noms des systèmes autonomes s'ouvre. Elle contient les informations concernant la première page de valeurs de systèmes autonomes.

3. Localisez chaque système autonome dont vous voulez personnaliser le nom :

- Pour changer le nombre de lignes de chaque page, utilisez l'option Nombre maximum par page.
- Pour afficher une autre page, utilisez les éléments de navigation situés au bas de la page.
- Pour effectuer une recherche, entrez une ou plusieurs chaînes de texte dans la zone de recherche, puis cliquez sur Rechercher.

Règles de correspondance :

- Les recherches ne respectent pas la casse.
- Toutes les chaînes de recherche spécifiées doivent être trouvées dans la colonne Numéro du système autonome ou Description.

- Entourez la chaîne de recherche de guillemets droits pour limiter la recherche à l'ordre et aux mots indiqués. Par exemple, les résultats obtenus pour la chaîne de recherche *site Internet* sans guillemets peuvent inclure *site Web Internet* et *site Web*.
4. Réviser les noms de systèmes autonomes qui s'affichent dans la colonne Description.
- Une fois que vous avez localisé un nom de système autonome par défaut qui doit être personnalisé, modifiez-le.

Modification de noms de systèmes autonomes

Personnalisez les noms de systèmes autonomes si nécessaire pour rendre les étiquettes des rapports d'interface plus conviviales.

Procédez comme suit :

1. (Facultatif) Réviser et corriger le paramètre Domaine si nécessaire.
Les noms de systèmes par défaut sont spécifiques du domaine. Les modifications des noms de systèmes autonomes affectent les rapports relatifs aux interfaces du domaine sélectionné.
2. Sélectionnez la ligne du numéro de système autonome que vous voulez modifier.
3. Cliquez sur Modifier.
La boîte de dialogue Modifier la description du numéro de système autonome s'ouvre.
4. Entrez le nom personnalisé (description) dans la zone Nouveau nom.
La valeur Ancien nom correspond au nom officiel (de base) du système autonome et vous ne pouvez pas la modifier.
5. Cliquez sur Enregistrer.
Le nom que vous avez spécifié s'affiche dans la colonne Description pour le numéro du système autonome sélectionné. Tous les noms de systèmes autonomes personnalisés sont affichés en gras.
Les noms de systèmes autonomes mis à jour apparaissent également dans des étiquettes et d'autres références dans les vues d'interfaces CA Network Flow Analysis suivantes :
 - Table du récapitulatif des tronçons suivants du système autonome (interface unique)
 - Graphiques à secteurs, graphiques de tendance et tables de récapitulatif des N principaux systèmes autonomes

6. Répétez ces étapes pour chaque système autonome que vous voulez personnaliser.

Remarque : Pour restaurer le nom officiel d'un système autonome, cliquez sur Réinitialiser dans la ligne appropriée, puis cliquez sur OK dans la zone de confirmation.

Nommage de routeurs

Vous pouvez changer les noms de routeur par défaut qui s'affichent dans la console NFA afin d'effectuer des corrections ou de rendre les noms plus explicites. Par défaut, le nom de routeur est l'adresse IP du routeur. Par exemple, vous voulez renommer un routeur pour que son nom corresponde à son emplacement géographique ou pour indiquer le type d'unité.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.
La page Interfaces actives s'ouvre et indique les routeurs actuels et leurs interfaces actives.
2. Cochez la case située à côté du routeur que vous voulez renommer.
3. Cliquez sur Modifier.
La boîte de dialogue Modifier le routeur s'ouvre.
4. Saisissez un nouveau nom de routeur dans la zone Nom.
5. Cliquez sur Enregistrer.
La boîte de dialogue Modifier le routeur se ferme. La page Interfaces actives affiche le nouveau nom de routeur.

Remarque : Pour restaurer le nom par défaut d'un routeur sélectionné, cliquez sur Réinitialiser dans la boîte de dialogue Modifier le routeur. Le lien Réinitialiser est affiché uniquement lorsque vous sélectionnez un routeur renommé.

Création de filtres de temps

Créez des filtres de temps pour permettre aux utilisateurs de créer des rapports contenant des données optimisées. Par exemple, vos utilisateurs veulent plusieurs rapports qui décrivent le trafic réseau durant les heures ouvrées. Vous créez un filtre de temps qui s'applique du lundi au vendredi, de 8:00 à 17:00 heures. Vous pouvez également créer des filtres de temps pour des périodes correspondant à des opérations dans votre environnement, comme les sauvegardes automatisées.

Vous pouvez également utiliser les filtres de temps pour configurer les interruptions de la page Configuration des interruptions.

Remarque : Pour obtenir des informations supplémentaires sur l'utilisation de filtres de temps, reportez-vous à la rubrique [Création d'interruptions](#) (page 107).

Les utilisateurs peuvent utiliser les filtres de temps personnalisés à partir de listes d'option de filtre de temps dans les emplacements suivants :

- Page Spécifier la planification de l'Assistant de création de rapports personnalisés ou de l'Assistant de création de rapports d'analyse.
- Options affichées par les opérateurs en cliquant sur le paramètre de période dans un rapport d'interface d'analyse en profondeur de types suivants : Présentation, Protocoles, Type de service, Hôtes, Conversations, Flux, Utilisation et Numéro du système autonome.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
2. Sous l'étiquette Administration : Génération de rapports du menu Administration, sélectionnez Filtres de temps.
La page Configuration du filtre de temps s'ouvre et affiche une liste des filtres de temps actuellement configurés.

3. Cliquez sur Ajouter.

La page Configuration du filtre de temps affiche les options permettant l'ajout d'un filtre de temps.

Configuration du filtre de temps

Ajouter un filtre d'heure

Nom du filtre de temps : *

Description :

le ☒ lundi ☒ mardi ☒ mercredi ☒ jeudi
☒ vendredi ☐ samedi ☐ dimanche

Heure de début 00 : 00 Heure de fin 00 : 00 (00:00 représente aussi bien le début que la fin du jour.)

* Champ obligatoire

4. Saisissez des valeurs dans les champs suivants :

- Nom du filtre de temps : définissez l'identificateur de filtre de temps, qui s'affiche dans les listes suivantes.
 - Liste de la page Configuration du filtre de temps (administrateurs)
 - Les options de filtre de temps disponibles dans la page Spécifier la planification de l'Assistant de création de rapports personnalisés.
 - Les options de filtre de temps disponibles lorsqu'un utilisateur ou l'administrateur clique sur le paramètre de période dans un rapport d'interface d'analyse en profondeur des types suivants : Présentation, Protocoles, Type de service, Hôtes, Conversations, Flux, Utilisation, et Numéro du système autonome.
- Description (facultatif) : ajoutez des informations pour identifier le filtre de temps qui s'affiche dans la liste des filtres de temps de la page Configuration du filtre de temps.
- le : acceptez les paramètres par défaut (du lundi au vendredi) ou sélectionnez d'autres jours pour les données de rapport de collecte.
- Heure de début et Heure de fin : acceptez les paramètres par défaut pour le début et la fin de la période quotidienne ou sélectionnez des paramètres personnalisés, au format 24 heures. Le paramètre par défaut de 00:00 à 00:00 inclut les données d'une période de 24 heures par jour.

Pour, par exemple, limiter la période de génération de rapports aux heures ouvrées, sélectionnez 08:00 comme heure de début et 17:00 comme heure de fin. Pour définir un filtre pour les sauvegardes qui s'exécutent le mardi de 23 heures à 03 heures du matin le mercredi, sélectionnez Mardi, puis 23:00 et 03:00.

5. Enregistrez le filtre de temps en cliquant sur l'un des boutons suivants :
 - Soumission terminée : enregistre le filtre de temps et renvoie à la liste de filtres de temps.
 - Soumettre et ajouter : enregistre le filtre de temps et continue d'afficher les options d'ajout pour que vous puissiez configurer un autre filtre de temps.

Remarque : Pour supprimer un filtre de temps, sélectionnez-le dans la liste de filtres de temps disponibles, cliquez sur Supprimer, puis confirmez la suppression lorsque vous y êtes invité. Pour modifier un filtre de temps, sélectionnez-le dans la liste de filtres disponibles, modifiez l'une des options affichées, puis cliquez sur Soumettre.

Création de périodes de génération de rapports

Créez des périodes de génération de rapports pour optimiser les résultats des rapports. Par exemple, vos utilisateurs analysent généralement le trafic réseau sur deux semaines. Pour faciliter l'affichage des données d'interface sur cette période, créez une période de génération de rapports de deux semaines.

Les périodes de génération de rapports personnalisées sont disponibles via l'option Période lorsqu'un utilisateur ou l'administrateur clique sur le paramètre de période dans un rapport d'interface d'analyse en profondeur des types suivants : Présentation, Protocoles, Type de service, Hôtes, Conversations, Flux, Utilisation et Numéro du système autonome. Pour plus d'informations sur ces types de rapport, consultez le *Manuel de l'utilisateur CA Network Flow Analysis*.

Procédez comme suit :

1. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
2. Sous l'étiquette Administration : Génération de rapports du menu Administration, sélectionnez Périodes de génération de rapports.
La page Configuration des périodes de génération de rapports s'ouvre et affiche une liste des périodes de génération de rapports actuelles, y compris les périodes de génération de rapports intégrées et personnalisées.
3. Cliquez sur Ajouter.
Les champs et les options permettant d'ajouter une période de génération de rapports sont affichés.

4. Spécifiez les valeurs suivantes :
 - Période de génération de rapports : identificateur de la période de génération de rapports qui s'affiche dans les listes de périodes de génération de rapports disponibles suivantes :
 - Liste de la page Configuration des périodes de génération de rapports (administrateurs)
 - Les options de période sont disponibles lorsqu'un utilisateur ou l'administrateur clique sur le paramètre de période dans un rapport d'interface d'analyse en profondeur des types suivants : Présentation, Protocoles, Type de service, Hôtes, Conversations, Flux, Utilisation et Numéro du système autonome.
 - Durée : nombre et type d'unités de temps (années, mois, semaines, jours ou heures).
 - Description (facultatif) : remarques supplémentaires pour faciliter l'identification de la période de génération de rapports. La description s'affiche dans la liste de la page Configuration des périodes de génération de rapports, mais uniquement pour les administrateurs.
5. Enregistrez la période de génération de rapports en cliquant sur l'un des boutons suivants :
 - Soumission terminée : enregistre la période de génération de rapports actuelle et renvoie à la liste de périodes de génération de rapports disponibles.
 - Soumettre et ajouter : enregistre la période de génération de rapports et continue d'afficher les options d'ajout pour que vous puissiez configurer une autre période.

Remarque : Pour supprimer une période de génération de rapports, sélectionnez-la dans la liste de périodes de génération de rapports disponibles, cliquez sur Supprimer, puis confirmez la suppression lorsque vous y êtes invité. Pour modifier une période de génération de rapports, sélectionnez-la dans la liste, modifiez l'une des options affichées, puis cliquez sur Soumettre.

Chapitre 5: Maintenance de CA Network Flow Analysis

Effectuez des opérations de maintenance sur CA Network Flow Analysis pour un fonctionnement optimal des fonctionnalités. Il est recommandé d'effectuer les tâches décrites dans les rubriques suivantes à intervalles réguliers. Par exemple, lorsqu'un utilisateur configure une interruption, l'administrateur doit la déployer.

Remarque : Pour effectuer les tâches décrites dans cette section, le rôle de votre compte d'utilisateur de console NFA doit être soit Administrateur soit Utilisateur avancé.

Ce chapitre traite des sujets suivants :

[Surveillance des composants CA Network Flow Analysis](#) (page 103)

[Création d'interruptions](#) (page 107)

[Configuration de destinations des interruptions](#) (page 110)

[Configuration des interruptions pour les outils de gestion des pannes externes](#) (page 112)

[Expiration des adresses caduques](#) (page 114)

[Gestion des services](#) (page 116)

Surveillance des composants CA Network Flow Analysis

Les services de surveillance vous permettent de surveiller les composants CA Network Flow Analysis. Les services de surveillance interrogent chaque serveur présents dans votre configuration CA Network Flow Analysis toutes les deux heures pour déterminer le statut de tous les composants. Vous pouvez établir des seuils, une adresse électronique pour la réception de messages et configurer d'autres paramètres pour que les services de surveillance vous notifie des problèmes rencontrés sur les composants dans les plus brefs délais.

Remarque : Pour obtenir des informations supplémentaires sur les services inclus sur chaque serveur de votre configuration CA Network Flow Analysis, consultez la rubrique [Gestion des services](#) (page 116).

Modification des paramètres du service de surveillance

Modifiez les paramètres de l'outil de surveillance pour modifier les valeurs de configuration comme les seuils, les paramètres d'interruption, les paramètres d'interrogation, l'adresse de notification et les chaînes de communauté.

Procédez comme suit :

1. Affichez la page Paramètres de l'outil de surveillance :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Intégrité : Paramètres de l'outil de surveillance.
La page de Paramètres de l'outil de surveillance s'ouvre et affiche les paramètres actuels.
2. Modifiez les paramètres du service de surveillance :

Chaîne de communauté

Chaîne SNMP utilisée pour identifier les composants dans un déploiement distribué. Les services de surveillance utilisent la chaîne de communauté pour la collecte d'informations à partir de Harvesters (et à partir de composants DSA dans un déploiement d'architecture à trois niveaux).

Par défaut : public

Seuil d'UC

Seuil d'utilisation de l'UC. Si l'adresse et la chaîne sont définies, vous recevez un courriel lorsque le seuil d'UC d'un serveur est dépassé et une notification d'interruption SNMP est générée.

Par défaut : 80 % d'utilisation de l'UC

Seuil du disque

Seuil d'utilisation du disque. Si l'adresse et la chaîne sont définies, vous recevez un courriel lorsque le seuil de disque d'un serveur est dépassé et une notification d'interruption SNMP est générée.

Par défaut : 80 % d'utilisation du disque

Adresse électronique

Adresse électronique du destinataire à utiliser pour les notifications en cas de dépassement des seuils. Pour informer plusieurs destinataires, séparez les adresses par des virgules. Le paramètre Adresse électronique n'a aucune valeur par défaut.

Par défaut : (aucun)

Seuil de la mémoire

Seuil d'utilisation de la mémoire. Si l'adresse et la chaîne sont définies, vous recevez un courriel lorsque le seuil de mémoire d'un serveur est dépassé.

Par défaut : 80 % d'utilisation de la mémoire

Nouvelles tentatives SNMP

Nombre de tentatives d'interrogation d'une unité SNMP. Selon la configuration de votre réseau, un nombre élevé de tentatives SNMP peut affecter les performances.

Par défaut : 2

Délai d'expiration SNMP

Nombre de secondes avant l'expiration d'une interrogation SNMP.

Par défaut : 5

Intervalle de contrôle du système

Nombre de minutes entre les vérifications du système par l'outil de surveillance.

Par défaut : 60

Chaîne de communauté d'interruptions

Chaîne SNMP à utiliser pour envoyer des interruptions.

Par défaut : public

Destination des interruptions

Adresse IP du serveur recevant les interruptions SNMP à partir des services d'outil de surveillance. Les interruptions sont générées lorsque des violations de seuil des performances des composants CA Network Flow Analysis se produisent.

Par défaut : (aucun)

3. Lorsque vous avez modifié les paramètres, cliquez sur Enregistrer.

Affichage du statut du système

Affichez la page Statut du système pour vérifier le statut global des composants CA Network Flow Analysis.

Procédez comme suit :

1. Affichez la page Statut du système :

- Dans le menu de console NFA, sélectionnez Administration.
- ou
- Dans le menu Administration, sélectionnez Statut du système.

La page Statut du système s'ouvre et affiche un aperçu rapide du statut des composants CA Network Flow Analysis. Les symboles de statut identifient les composants pour lesquels des avertissements ont été générés. Le nombre d'avertissements s'affiche entre parenthèses après l'étiquette de composant.

2. Cliquez sur un composant affichant un symbole d'avertissement pour consulter les détails.

Une table d'avertissements s'affiche.

Adresse	Heure	Type	Informations
			Composant de collecte - Dernier horodatage de l'outil de traitement des fichiers de collecte : 15,7 minutes avant le contrôle
10.0.12.58	13/08/2012 09:15 CEST	Mémoire	L'utilisation de la mémoire est inconnue.
10.0.12.58	13/08/2012 09:15 CEST	UC	L'utilisation de l'UC est inconnue.
10.0.12.58	13/08/2012 09:15 CEST	Disque	L'utilisation du disque est inconnue.
10.0.12.58	13/08/2012 09:15 CEST	Service	L'état actuel du service de SNMP est Arrêté.

3. Vérifiez chaque avertissement pour chaque composant.

Création d'interruptions

Créez des interruptions pour informer les gestionnaires de réseau lorsque certains événements se produisent. Les administrateurs peuvent créer des interruptions et doivent déployer toutes les interruptions créées par les utilisateurs.

Vous pouvez [intégrer des interruptions CA Network Flow Analysis à des packages de gestion des pannes externes](#) (page 112).

Procédez comme suit :

1. Affichez la page Ajouter une définition d'interruption :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Alertes.
La page Configuration des interruptions s'ouvre et affiche la liste des interruptions actuelles.
 - c. Cliquez sur Ajouter.
La page Ajouter une définition d'interruption s'ouvre.
2. Saisissez une description et définissez les interfaces que l'interruption surveille :
 - Description : identifie la nouvelle interruption. Saisissez des informations sur le protocole et le seuil, comme Surveillance de l'utilisation de Microsoft SQL au-dessus de 65%.
 - Sélectionner une interface ou Sélectionner un groupe d'interfaces : lien vers un index d'interfaces ou de groupes d'interfaces, que vous utilisez pour sélectionner les interfaces surveillées par l'interruption.

Remarque : Si l'interface ou le groupe d'interfaces associé est supprimé après le déploiement de l'interruption, une erreur Groupe d'interfaces inconnu se produira. Pour éliminer cette erreur, associez l'interruption à une interface ou à un groupe d'interfaces différent.
3. (Facultatif) Créez une interruption basée sur l'utilisation en fournissant les informations suivantes :
 - Bouton radio Seuils : Utilisation : permet de définir le seuil de l'interruption sur l'utilisation. Utilisez les champs contextuels qui sont ajoutés pour ce type d'interruption.
 - Champ Utilisation : En entrée : pourcentage de l'utilisation qui correspond à la valeur de seuil en entrée.
 - Liste Utilisation : En entrée : Minutes : nombre de minutes pour la violation de seuil en entrée qui génère une interruption.

- Champ Utilisation : En sortie : pourcentage de l'utilisation qui correspond à la valeur de seuil en sortie.
 - Liste Utilisation : En sortie : Minutes : nombre de minutes pour la violation de seuil en sortie qui génère une interruption.
 - Protocole : protocole pour le trafic surveillé. Dans la boîte de dialogue Index de protocole qui s'ouvre, sélectionnez le protocole. L'interruption s'appliquera au protocole et aux interfaces sélectionnées.
 - Type de service (facultatif) : type de service (ToS) du trafic surveillé. L'interruption s'appliquera aux interfaces, au protocole et au type de service sélectionnés. Pour surveiller l'ensemble du trafic des différents types de service, sélectionnez Tout.
 - Filtre de temps (facultatif) : période de la surveillance, si vous choisissez de la limiter de cette façon. Sélectionnez un des filtres de temps de la liste. La liste Filtre de temps inclut tous les filtres de temps créés par l'administrateur.
4. (Facultatif) Créez une interruption basée sur le taux en fournissant les informations suivantes :

Par exemple, vous créez une interruption basée sur le taux et établissez des seuils aussi bien pour le trafic entrant que pour le trafic sortant. L'interruption est déclenchée lorsque le seuil est dépassé lors de la période définie.

- Seuils : Taux : permet de définir le seuil de l'interruption sur le taux de transfert. Utilisez les champs contextuels qui sont ajoutés pour ce type d'interruption.
- Taux : En entrée : vitesse de transfert des données en entrée qui correspond à la valeur de seuil. Définissez le nombre de bits, de kilobits, de mégabits ou de gigabits par seconde, en fonction de l'unité de mesure sélectionnée.
- Taux : Unités de mesure : unité de mesure pour le transfert de données. Sélectionnez Bits par seconde (bits/s), Kilobits par seconde (Kbits/s), Mégabits par seconde (Mbits/s) ou Gigabits par seconde (Gbits/s).
- Taux : En entrée : Minutes : nombre de minutes pour la violation de seuil en entrée qui génère une interruption.
- Taux : En sortie : seuil pour le transfert de données en sortie. Entrez le nombre de bits, de kilobits, de mégabits ou de gigabits par seconde, en fonction de l'unité de mesure sélectionnée pour le seuil en entrée.
- Taux : En sortie: Minutes : nombre de minutes pour la violation de seuil en sortie qui génère une interruption.
- Protocole : protocole pour le trafic surveillé. Dans la boîte de dialogue Index de protocole qui s'ouvre, sélectionnez le protocole. L'interruption s'appliquera au protocole et aux interfaces sélectionnées.

- Type de service (facultatif) : type de service (ToS) du trafic surveillé. L'interruption s'appliquera aux interfaces, au protocole et au type de service sélectionnés. Pour surveiller l'ensemble du trafic des différents types de service, sélectionnez Tout.
 - Filtre de temps (facultatif) : période de la surveillance, si vous choisissez de la limiter de cette façon. Sélectionnez un des filtres de temps de la liste. La liste Filtre de temps inclut tous les filtres de temps créés par l'administrateur.
5. (Facultatif) Créez une interruption basée sur le volume en fournissant les informations suivantes :
- Seuils : Volume : permet de définir le seuil de l'interruption sur le volume de données. Utilisez les champs contextuels qui sont ajoutés pour ce type d'interruption.
 - Volume : En entrée : volume de données en entrée qui correspond à la valeur de seuil. Définissez le nombre d'octets, de kilo-octets, de mégaoctets ou de gigaoctets, en fonction de l'unité de mesure sélectionnée.
 - Volume : Unités de mesure : unité de mesure pour le transfert de données. Sélectionnez Octets, Kilo-octets (ko), Mégaoctets (Mo), Gigaoctets (Go) ou Téraoctets (To).
 - Volume : En sortie : volume de données en sortie qui correspond à la valeur de seuil. Entrez le nombre d'octets, de kilo-octets, de mégaoctets ou de gigaoctets, en fonction de l'unité de mesure sélectionnée pour le seuil en entrée.
 - Volume : En sortie: Minutes : nombre de minutes pour la violation de seuil en sortie qui génère une interruption.
 - Protocole : protocole pour le trafic surveillé. Dans la boîte de dialogue Index de protocole qui s'ouvre, sélectionnez le protocole. L'interruption s'appliquera au protocole et aux interfaces sélectionnées.
 - Type de service (facultatif) : type de service (ToS) du trafic surveillé. L'interruption s'appliquera aux interfaces, au protocole et au type de service sélectionnés. Pour surveiller l'ensemble du trafic des différents types de service, sélectionnez Tout.
 - Filtre de temps (facultatif) : période de la surveillance, si vous choisissez de la limiter de cette façon. Sélectionnez un des filtres de temps de la liste. La liste Filtre de temps inclut tous les filtres de temps créés par l'administrateur.
6. (Facultatif) Créez une interruption basée sur le flux en fournissant les informations suivantes :
- Seuils : Flux : permet de définir le seuil de l'interruption sur le nombre de flux. Utilisez les champs contextuels qui sont ajoutés pour ce type d'interruption.
 - Flux : Total : nombre de flux entrants qui correspond à la valeur de seuil. Définissez le nombre de flux par minute (unités, milliers, millions, etc.) selon l'unité de mesure sélectionnée.

- Flux : Unités de mesure : unité de mesure pour le transfert de données. Sélectionnez Flux/minute, Milliers de flux/minute ou Millions de flux/minute.
- Flux : Minutes : nombre de minutes pour la violation de seuil qui génère une interruption.
- Filtre de temps (facultatif) : période de la surveillance, si vous choisissez de la limiter de cette façon. Sélectionnez un des filtres de temps de la liste. La liste Filtre de temps inclut tous les filtres de temps créés par l'administrateur.

7. Lorsque vous avez effectué vos sélections, cliquez sur Soumettre.

L'interruption est déployée.

Remarque : Les interruptions sont envoyées à la destination définie dans les paramètres d'application.

Pour supprimer une définition d'interruption, cliquez sur sa description dans la liste des interruptions de la page Configuration des interruptions. Cliquez sur le bouton Supprimer qui s'affiche en mode Modifier. Vérifiez la suppression lorsque vous y êtes invité.

Pour modifier une définition d'interruption, cliquez sur sa description dans la liste des interruptions de la page Configuration des interruptions. Effectuez les mises à jour dans la page Configuration des interruptions en mode Modifier. Cliquez sur Soumettre. L'interruption est mise à jour.

Configuration de destinations des interruptions

Configurez des destinations pour les interruptions [créées](#) (page 107) par vous et des opérateurs CA Network Flow Analysis.

- Pour afficher des interruptions en tant qu'événements dans la console CA Performance Center, définissez la destination des interruptions dans la page Paramètres de l'application.
- Si vous voulez également générer des interruptions de l'outil de surveillance, configurez la destination des interruptions dans la page Paramètres de l'outil de surveillance de la console NFA.

Pour permettre l'affichage des interruptions dans la console CA Performance Center, procédez comme suit :

1. Affichez la page Paramètres de l'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu situé à gauche, sélectionnez Paramètres de l'application.
La page Paramètres de l'application s'ouvre et contient les valeurs de configuration actuelles.

2. Recherchez le champ Destination des interruptions au bas de la page.
3. Vérifiez que la valeur Destination des interruptions corresponde à l'adresse IP du serveur de la console NFA enregistrée dans CA Performance Center.

Par exemple, veillez à ce que l'adresse IP de la destination des interruptions corresponde à la valeur Nom d'hôte dans CA Performance Center. Si l'adresse IP de l'hôte n'est pas incluse dans le nom de la source de données CA Performance Center, vérifiez la valeur Nom d'hôte de la manière suivante :

Connectez-vous à la console CA Performance Center. Sélectionnez Administration, Sources de données. Dans la page de gestion des sources de données, cliquez avec le bouton droit de la souris sur la source de données CA Network Flow Analysis et sélectionnez Modifier dans le menu. Dans la boîte de dialogue Modifier la source de données qui s'ouvre, vérifiez la valeur Nom d'hôte.

Pour définir la destination des interruptions de l'outil de surveillance, procédez comme suit :

1. Affichez la page Paramètres de l'outil de surveillance :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu situé à gauche, sélectionnez Paramètres de l'outil de surveillance.
La page de Paramètres de l'outil de surveillance s'ouvre et affiche les paramètres actuels.
2. Vérifiez que les paramètres de l'outil de surveillance sont corrects, y compris la destination des interruptions :

Saisissez l'adresse IP du serveur qui héberge le récepteur d'interruptions. Les services de surveillance enverront des interruptions SNMP à l'adresse de destination des interruptions.

Pour plus d'informations sur les autres paramètres de l'outil de surveillance, reportez-vous à la rubrique [Modification des paramètres du service de surveillance](#) (page 104).
3. Lorsque vous avez modifié les paramètres, cliquez sur Enregistrer.
Les paramètres sont enregistrés. Les messages seront envoyés pour toute nouvelle interruption générée.

Tâches facultatives supplémentaires :

- Vérifiez que les événements sont affichés dans la page Affichage des événements de CA Performance Center. Si la page Affichage des événements n'indique pas les événements prévus, vérifiez que les conditions suivantes sont remplies :
 - Les fichiers affichent les événements qui ont été générés et qui ont été envoyés au gestionnaire d'événements.
 - Le nom d'hôte du gestionnaire d'événements peut être résolu par le serveur DNS pour CA Network Flow Analysis.
 - Dans la page Paramètres de l'application de la console NFA, la valeur Destination des interruptions correspond à l'adresse IP du serveur de la console NFA enregistrée en tant que source de données pour CA Performance Center.
- [Configuration des interruptions pour l'utilisation d'outils externes](#) (page 113)

Configuration des interruptions pour les outils de gestion des pannes externes

Vous pouvez intégrer les interruptions que CA Network Flow Analysis génère à d'autres outils de gestion de réseau. Les interruptions fournissent les informations suivantes, qui peuvent être utiles dans d'autres outils :

- L'interface affectée par le seuil
- Le protocole affecté par le seuil
- La direction du trafic affecté par le seuil (entrée, sortie ou les deux)
- Le seuil dépassé (par exemple, 1,23 Mo/s)
- Le trafic réel observé qui a déclenché l'interruption (par exemple, 1,30 Mo/s).
- Si la notification indique une nouvelle violation de seuil observée ou une violation de seuil effacée. Pour une violation de seuil effacée, le motif de l'effacement est inclus. Les motifs sont :
 - Le taux est retombé en dessous du seuil.
 - Aucune donnée n'a été détectée au cours de la dernière période.
 - Un filtre de temps a empêché l'inclusion des données.

Configuration des interruptions CA Network Flow Analysis pour les outils externes

Configurez des interruptions CA Network Flow Analysis pour regrouper des événements dans les outils externes et leur fournir des données utiles.

Procédez comme suit :

1. Accédez au fichier MIB.

La base de données d'informations de gestion (MIB) contient les informations relatives au contenu des interruptions envoyées par CA Network Flow Analysis. Le fichier MIB se trouve dans le répertoire suivant :

`<chemin_installation_NFA>\reporter\MIB.`

2. Compilez la MIB dans votre outil de gestion de réseaux et configurez-le pour que les interruptions CA Network Flow Analysis correspondent logiquement.

Une interruption est envoyée lorsque le programme détecte une nouvelle violation de seuil et lorsque la condition est supprimée. Configurez votre outil de gestion de réseaux pour regrouper ces deux événements, de façon à supprimer la condition d'avertissement lorsque le programme envoie l'interruption de condition d'effacement. Pour effectuer le regroupement, configurez l'outil pour qu'il vérifie les valeurs suivantes dans la base de données d'informations de gestion :

- NetQoSTrafficFlowEntry
- NetQoSTrafficFlowDataEventStart, qui indique une nouvelle interruption.
- NetQoSTrafficFlowDataEventStop, qui indique que l'interruption a été effacée.

Pour plus d'informations sur la définition de règles pour la gestion intelligente des interruptions, consultez la documentation de votre outil de gestion de réseaux.

3. Créez et déployez des interruptions CA Network Flow Analysis, si vous ne l'avez pas déjà fait, comme décrit dans la section [Création d'interruptions](#) (page 107).
4. Vérifiez que la destination d'interruption contient l'adresse IP du serveur utilisé pour installer l'outil de gestion des pannes.

Les interruptions sont envoyées à la destination définie dans les paramètres d'application.

Dépannage des problèmes liés aux interruptions intégrées

Vérifiez les paramètres d'interruption pour corriger les problèmes rencontrés au niveau des données d'interruption CA Network Flow Analysis reçues par les outils de gestion des pannes externes.

Procédez comme suit :

1. Vérifiez que la destination d'interruption est définie sur l'adresse IP du serveur utilisé pour installer l'outil de gestion des pannes.
2. Vérifiez que les interruptions sont configurées correctement. Pour plus d'informations, consultez la rubrique [Création d'interruptions](#) (page 107).

Si vous avez vérifié ces paramètres, mais qu'aucune interruption n'est reçue comme prévu, contactez le support CA pour obtenir de l'aide.

Expiration des adresses caduques

Les adresses IP peuvent automatiquement être affectées à l'aide du protocole DHCP et peuvent expirées. Vous pouvez définir l'expiration d'adresses IP caduques (obsolètes) pour planifier leur actualisation. Vous pouvez également modifier la fréquence des mises à jour de nom DNS lorsque vous modifiez une adresse.

Le programme vérifie le serveur DNS et actualise le nom DNS pour chaque adresse expirée.

Procédez comme suit :

1. Affichez la page Configuration de l'adresse ou du nom d'hôte :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu de la page Administration, sélectionnez Génération de rapports : Adresses.
La page Configuration de l'adresse ou du nom d'hôte s'ouvre :
2. (Environnement à domaines multiples uniquement) : sélectionnez le domaine qui contient l'adresse à actualiser.
3. Cliquez sur Liste.
Une liste s'ouvre et affiche les adresses pour le domaine sélectionné.

4. Cochez la case située à côté de chaque adresse que vous voulez marquer comme expirée.
5. Cliquez sur Expirer, puis confirmer l'expiration lorsque l'invite s'ouvre.

L'actualisation de la résolution DNS des adresses sélectionnées est planifiée. Le processus d'actualisation est généralement exécuté dans les 5 minutes.

Gestion des services

Vous pouvez démarrer ou arrêter des services CA Network Flow Analysis ou vérifier le statut d'un service dans la fenêtre Services Windows.

Les services CA Network Flow Analysis sont décrits brièvement dans la liste suivante. Si les composants CA Network Flow Analysis sont installés sur plusieurs serveurs, les services s'exécutent sur chaque serveur, comme illustré dans la liste suivante. Si tous les composants sont installés sur un système autonome, tous les services s'exécutent sur le serveur autonome.

- *Services Web de collecte et d'interrogation de CA NFA* : fournit des interfaces de service Web pour la console NFA afin de permettre les communications avec le Harvester et l'interrogateur (serveurs autonome ou de Harvester).

Harvesters Linux : NFA CollpollWS (nfa_collpollws)

- *Conservation de données CA NFA* : gestion de la suppression pour appliquer les limites établies de conservation des fichiers de données en fonction des délais et du volume.
 - Déploiement autonome ou distribué à 2 niveaux : gestion de la suppression de données de résolution en 15 minutes, 1 minute et des données d'examen des flux (serveurs autonomes et de Harvester).
 - Déploiement à 3 niveaux : gestion de la suppression des données de résolution en 1 minute et des données d'examen de flux sur des serveurs de DSA et des données de résolution en 15 minutes sur les serveurs de Harvester (serveurs de DSA).

Harvesters Linux : NFA Dataretention (nfa_dataretention)

- *proxys DNS/SNMP CA NFA* : gestion des demandes SNMP et DNS à partir de l'interrogateur (tous les serveurs).

Harvesters Linux : NFA Proxies (nfa_proxies)

- *CA NFA DSALoader* : traitement des données de résolution en 15 minutes dans des fichiers RTR pour le stockage (architecture à trois niveaux). Convertit également les fichiers RTR en fichiers RTR15 pendant la migration vers l'architecture à 2 niveaux (serveurs de DSA).

- *Serveur de fichiers CA NFA* :

- Déploiement distribué ou autonome à deux niveaux : collecte des fichiers de données EOVS sur les serveurs de Harvester pour permettre à la console NFA de les récupérer (serveurs de Harvesters ou autonomes).
- Déploiement à 3 niveaux : collecte des fichiers de données EOVS sur les serveurs de Harvester pour permettre à la console NFA de récupérer et de copier les fichiers de données historiques sur le serveur de la console NFA pour chaque DSA à récupérer (serveurs de Harvester et de console NFA).

Harvesters Linux : NFA Filewebservice (nfa_filewebservice)

- *Composant Harvester de CA NFA* : exécution du Harvester/processus de collecte (serveurs autonomes et de Harvester).

Harvesters Linux : NFA Harvester (nfa_harvester)

- *Authentification unique CA Performance Center* : exécution du logiciel d'authentification unique qui permet aux utilisateurs de naviguer entre CA Performance Center et CA Network Flow Analysis sans devoir se réauthentifier.

- *Interrogateur de CA NFA* : exécution de l'interrogateur, récupération des listes d'interfaces à partir des routeurs et gestion du mappage des ID d'interface persistants (serveurs de Harvesters et autonomes).

Harvesters de Linux : interrogateur NFA (nfa_poller)

- *Service de pompage de CA NFA* : déplacement des fichiers EOVS et des fichiers de données historiques des serveurs de Harvester à la console NFA (serveurs de DSA).
- *Reaper de CA NFA* : exécution du processus du Reaper qui traite les flux entrants et écrit les fichiers sortants pour les données de résolution en 1 minute, 15 minutes ou pour les données de présentation de l'entreprise (serveurs de Harvester).

Harvesters Linux : service de Reaper de CA NFA (nfa_reaper)

- *Source de la base d'informations de génération de rapports CA NFA* : interface statique permettant à CA Performance Center d'obtenir les données CA Network Flow Analysis pour les vues et les tableaux de bord CA Performance Center (serveurs de console NFA et autonomes).

- *NetQoS MySQL1* : exécution de l'instance MySQL standard sur le port 3308 et stockage des données de configuration MySQL (tous les serveurs).

- *NQMySQL1 NetQoS* : exécution du moteur de stockage personnalisé qui stocke les fichiers pour les données de résolution en 1 minute, en 15 minutes et les données d'examen des flux (tous les serveurs).

Harvesters Linux : CSE MySQL (nfa_mysqlCSE)

- *Service de gestionnaire NetQoS Reporter* : gestion des processus de synchronisation des éléments entre les bases de données de la console NFA et du Harvester, tels que les profils SNMP (serveurs de console NFA et autonomes).

- *Services généraux NetQoS Reporter/Analyzer* : gestion de plusieurs tâches, y compris la gestion des licences, la détection des interfaces inactives, la gestion planifiée des rapports d'analyse et personnalisés et le déclenchement des interruptions (serveurs de console NFA et autonomes).

- *Service de pompage de NetQoS Reporter/Analyzer* : récupération des données de l'entreprise à partir du Harvester (serveurs de console NFA et autonomes).

- *Services de requête de NetQoS Reporter/Analyzer* : interfaces d'exécution de rapports personnalisés et de rapports d'analyse immédiats (serveurs de console NFA et autonomes). Tâches incluses :

- Groupes automatiques : effectuez la maintenance des groupes contrôlés par le système et de leurs membres.

- DNS : effectuez une résolution DNS inversée pour fournir les noms des hôtes des adresses IP.
- Maintenance : collectez les données, déployez les paramètres sur les serveurs de Harvester et d'autres serveurs, et effectuez d'autres tâches.
- *Service de rapports de NetQoS Reporter/Analyzer* : interfaces d'exécution des rapports d'examen de flux et des rapports personnalisés planifiés (serveurs de console NFA et autonomes).
- *Outil de surveillance de NetQoS Reporter/Analyzer* : composants d'interrogation pour les informations de statut (serveurs de console NFA et autonomes).

Journaux de services

Les journaux de services sont décrits dans le tableau suivant et sont identifiés par leurs noms sur les serveurs Windows et Linux. La partie initiale de chaque chemin correspond au chemin d'installation de CA Network Flow Analysis, comme les emplacements par défaut : C:\CA\NFA sur un serveur Windows ou /opt/CA/NFA sur un serveur de Harvester Linux. Le tableau répertorie également les noms et les emplacements des fichiers journaux associés aux services, ainsi que tous les fichiers de configuration disponibles pour contrôler la configuration du niveau de journalisation.

informations des services/journaux	Autonome	Harvester	Console	DSA
Services Web de collecte et d'interrogation de CA NFA (Linux : nfa_collpollws) Journal : \Netflow\Logs\collpollws-wrapper.log	Oui	Oui		
Conservation de données CA NFA (Linux : nfa_dataretention) Journal : \Netflow\Logs\dataretention-wrapper.log	Oui	Oui		Oui
Proxys DNS/SNMP CA NFA (Linux : nfa_proxies) Journal : \Netflow\Logs\proxies-wrapper.log	Oui	Oui	Oui	Oui
CA NFA DSALoader Journal : \Netflow\Logs\dsaLoaderErrors-<aaa-mm-jj>.log				Oui
Serveur de fichiers CA NFA (Linux : nfa_filewebsevice) Journal : \Netflow\Logs\fileserver-wrapper.log	Oui	Oui	Oui (3 niveaux)	
Harvester CA NFA (Linux : nfa_harvester) Journal : \Netflow\Logs\harvester-wrapper.log	Oui	Oui		
Interrogateur CA NFA (Linux : nfa_poller) Journal : \Netflow\Logs\poller-wrapper.log	Oui	Oui		
Service de pompage CA NFA Journal : \Netflow\logs\pumpservice-wrapper.log				Oui

informations des services/journaux	Autonome	Harvester	Console	DSA
Reaper CA NFA (Linux : nfa_reaper) Journal : \Netflow\Logs\RealtimeReaperErrors<aaaa-mm-jj>.log		Oui		
Source de la base d'informations de génération de rapports de CA NFA Journal : \Reporter\RIB\NFA\webapps\NFARS\WEB-INF\logs\application.log	Oui		Oui	
Service Web de proxy DNS Journal : \ProxyServices\Logs\DnsProxyWSLog<aaaa-mm-jj>.log Configuration du niveau de journalisation (console NFA uniquement) : \ProxyServices\Web.config <add key="LogLevel" value="6"/> Valeur par défaut : 4	Oui		Oui	
NetQoS MySql51 (Linux : mysql51) Journal : \MySql51\data<nom_serveur>.err	Oui	Oui	Oui	Oui
NetQoS NQMySql51 (Linux : nfa_mysqlCSE) Journal : \Netflow\Logs\oursql_5.1_error.log	Oui	Oui	Oui	Oui
Service de gestionnaire de NetQoS Reporter Journal : \Reporter\Logs\Manager Service Log<aaaa-mm-jj>.log Paramètre du niveau de journalisation : \Reporter\ReporterAnalyzer.ManagerService\bin\ReporterManagerService.exe.config <setProperties Severity="6" /> Valeur par défaut : 4	Oui		Oui	
Services généraux de NetQoS Reporter/Analyzer Journal : \Reporter\Logs\nqservErrors<aaaa-mm-jj>.log	Oui		Oui	
Service de pompage de NetQoS Reporter/Analyzer Journal : \Reporter\Logs\PumpLog<aaaa-mm-jj>.log Configuration du niveau de journalisation : \Reporter\NetQoS.ReporterAnalyzer.PumpService\bin\NetQoS.ReporterAnalyzer.PumpService.exe.config <setProperties Severity="6" /> Valeur par défaut : 4	Oui		Oui	
Services de requête NetQoS ReporterAnalyzer (services de génération de rapports) Journal de tâche de groupes automatiques : \Reporter\Logs\ManagerService_AutomaticGroupsLog<aaaa-mm-jj>.log Journal de tâche DNS : \Reporter\Logs\ManagerService_DnsLog<aaaa-mm-jj>.log Journal de tâches de maintenance : \Reporter\Logs\ManagerService_MaintenanceLog<aaaa-mm-jj>.log	Oui		Oui	

informations des services/journaux	Autonome	Harvester	Console	DSA
Service de rapport de NetQoS Reporter/Analyzer Journal (journal d'examen des flux) : \Reporter\Logs\ReportServiceLog<aaaa-mm-jj>.log Configuration du niveau de journalisation : \Reporter\NetQoS.ReporterAnalyzer.ReportService\ bin\NetQoS.ReporterAnalyzer.ReportService.exe.config <setProperties Severity="6" /> Valeur par défaut : 4 Pour journaliser chaque interrogation en plus de la journalisation d'événement standard : <add key="VerboseLogging" value="True"/>	Oui		Oui	
Outil de surveillance de NetQoS Reporter/Analyzer Journal : \Reporter\Logs\WatchdogLog<aaaa-mm-jj>.log Configuration du niveau de journalisation : \Reporter\ NetQoS.ReporterAnalyzer.WatchdogService\bin\ WatchdogService.exe.config <setProperties Severity="6" /> Valeur par défaut : 4	Oui		Oui	

Chapitre 6: Administration avancée

Les rubriques suivantes décrivent toutes les tâches que vous pouvez effectuer à l'aide des fonctions d'administration, notamment l'installation, la configuration et la personnalisation.

Ce chapitre traite des sujets suivants :

[Mappage d'applications](#) (page 121)

[Utilisation des places réservées](#) (page 128)

[Utilisation des interfaces](#) (page 131)

[Modification d'adresses IP de DSA](#) (page 136)

Mappage d'applications

Vous pouvez rassembler le trafic d'une application qui utilise plusieurs ports sur un seul port. Le mappage du trafic d'application vers un port unique facilite la génération de rapports relatifs au trafic total de l'application. Pour créer des mappages d'applications, utilisez les fonctions d'administration :

- Définissez des règles de mappage pour cumuler ou répartir les données selon le numéro de port.
- Configurez des paramètres globaux pour la prise en charge des règles de mappage dans les rapports.

Par exemple, vous voulez mapper le trafic vers un port cible dans les situations suivantes :

- Différenciez les protocoles communs basés sur le type d'application. Par exemple, vous pouvez différencier les protocoles HTTP d'un CRM, des portails Web et du trafic Internet.
- Cumulez le trafic de VoIP utilisant plusieurs ports différents dans un seul port. Vous pouvez cumuler tout le trafic de VoIP avec un bit de type de service approprié et le mapper vers un port unique pour l'identifier dans les rapports.
- Cumulez tout le trafic de courriel pour les systèmes de messagerie qui utilisent plusieurs protocoles, comme IMAP et POP. Vous pouvez inclure dans les rapports tout le trafic IMAP et POP d'un groupe principal de serveurs en tant qu'application unique dans un port. Par exemple, les courriels IMAP utilisent le port TCP 443 et les courriels POP les ports TCP 109 et 100. Vous mappez tout le courriel vers le port 31000 et l'étiquetez *Courriel*.
- Identifiez tout le trafic Microsoft Exchange Server qui utilise une large plage de numéros de port. Vous pouvez mapper le trafic vers un port unique et l'étiqueter comme *MS Exchange*.

Priorités de mappage

Vous pouvez utiliser des règles d'administration pour identifier le type de trafic à mapper vers un port cible. Tous les paquets qui correspondent aux critères spécifiés sont mappés vers le port cible. Vous pouvez identifier le trafic à mapper selon le type de service ou par une combinaison de protocole avec la plage de sous-réseau/port ou de serveur/port/type de service. La combinaison de valeurs spécifiée est comparée à l'en-tête IP de chaque paquet.

Les priorités suivantes s'appliquent au mappage d'applications lorsque les règles entrent en conflit. Une règle à la priorité lorsque ses critères sont supérieurs aux critères d'une autre règle.

- *Priorité 1* : les critères de port d'hôtes et de sources sont définis (règle d'hôte).
Exemple de trafic à surveiller : une application sur un serveur.
- *Priorité 2* : le type de service est défini (toutes les règles).
Exemple de trafic à surveiller : le type de service spécifié.
- *Priorité 3* : le port est défini, mais le port de source ne l'est pas (règle d'hôte).
Exemple de trafic à surveiller : le trafic de serveur.
- *Priorité 4* : le sous-réseau est défini (règle de sous-réseau).
Exemple de trafic à surveiller : le trafic généré à partir d'un réseau ou d'une application.

Configuration des paramètres globaux pour le mappage d'applications

Vérifiez les paramètres globaux qui affectent les mappages d'applications. Effectuez les modifications nécessaires pour personnaliser le comportement des mappages d'applications. Les paramètres globaux qui affectent le mappage d'applications incluent les options suivantes :

- *Port de redirection TCP* : port cible pour le trafic TCP redirigé. Le trafic TCP qui ne doit pas accéder au port de mappage d'applications cible est redirigé vers le port de redirection TCP.
- *Masque du type de service* : détermine si tous les bits de type de service sont utilisés pour les valeurs de type de service.
- *Port de redirection UDP* : port cible pour le trafic UDP redirigé, comme pour le paramètre de port de redirection TCP.
- *Conserver le protocole de mappage ToS* : détermine si les valeurs de protocole sont incluses dans les rapports en plus des valeurs de type de service.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Définitions d'application.
La page Définitions d'application s'affiche.
2. Cliquez sur Paramètres supplémentaires.
La page Paramètres de l'application s'affiche.
3. Vérifiez et corrigez les paramètres globaux qui affectent les mappages d'applications :
 - *Port de redirection TCP* : port alternatif à utiliser pour le trafic qui ne correspond pas aux règles de mappage d'applications pour le port cible d'origine.

Par exemple, vous mappez tout le trafic HTTP de vos serveurs de portail Web vers le port TCP 65550 et vous avez défini la valeur de port de redirection TCP sur 63000. Le port 65550 est réservé pour le trafic HTTP, donc le trafic non HTTP qui devrait normalement transiter par ce port 65550 est redirigé vers le port 63000.
 - *Masque du type de service* : limite les valeurs de type de service de 8 bits incluses dans les rapports pour les flux. La valeur par défaut pour ce paramètre est 255, ce qui correspond à l'activation de tous les bits de type de service.
 - *Port de redirection UDP* : port qui redirige le trafic non UDP, comme pour le paramètre de port de redirection TCP.
 - *Conserver le protocole de mappage ToS* : détermine si les valeurs de protocole sont incluses dans les rapports en plus des valeurs de type de service. O (Oui) conserve les protocoles utilisés et les données de types de service sont incluses dans les rapports séparément. N (Non) affiche les valeurs de type de service pour le trafic, mais pas les protocoles impliqués. Le paramètre par défaut est O.
4. Cliquez sur Enregistrer.

Vos modifications sont enregistrées. La page Paramètres de l'application reste affichée.

Création d'une règle de mappage d'applications de sous-réseau

Créez une règle d'application de sous-réseau pour regrouper le trafic généré à partir d'un sous-réseau et d'un masque. La règle d'application permet aux utilisateurs d'inclure facilement dans les rapports le trafic total correspondant à une application.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Définitions d'application.
La page Définitions d'application s'affiche.
2. Vérifiez que Mappage d'applications est la valeur sélectionnée pour Règles.
3. Cliquez sur Ajouter une règle.
La boîte de dialogue Ajouter un mappage d'applications s'ouvre.
4. Vérifiez que Sous-Réseau est sélectionné comme type de règle dans la partie supérieure de la boîte de dialogue. Cette option est sélectionnée par défaut.
La boîte de dialogue Ajouter un mappage d'applications affiche les options pour une règle de mappage d'applications de sous-réseau.
5. Saisissez des valeurs pour les paramètres suivants :
 - Sous-réseau : adresse IP de la source de données, au format décimal séparé par des points. Pour spécifier un sous-réseau qui correspond à toutes les adresses, utilisez 0.0.0.0/0 comme sous-réseau et comme masque.
 - Masque : masque à appliquer au sous-réseau.
 - Protocole : protocole des données qui seront affectées par la règle (TCP ou UDP).
 - Port de début : port de début de la plage de ports pour la collecte de données, au format décimal de base 10. Le port de début est inclus dans la plage de ports. La valeur de port maximum permise est 65535.
 - Port de fin : dernier port de la plage à utiliser pour la collecte de données. Le port de fin est inclus dans la plage de ports.
 - Port de destination : port cible qui collectera les données mappées.
 - Nom : identificateur de la règle tel qu'elle est répertoriée dans la page Définitions d'application.
 - Description (facultatif) : texte descriptif complémentaire permettant d'identifier le type de règle et son utilisation.

Remarque : Si plusieurs règles de mappage d'applications ont les mêmes paramètres de destination de port et de protocole, elles portent le même nom.

6. Lorsque les valeurs sont correctes pour tous les champs requis, cliquez sur Enregistrer.

La boîte de dialogue Ajouter un mappage d'applications se ferme. La nouvelle règle est incluse dans la liste des règles de mappage d'applications.

7. (Facultatif) Lancez des rapports pour vérifier que tout le trafic sur le port cible correspond à la règle.
8. (Facultatif) Une fois que vous avez constaté les effets du mappage d'applications créé ou modifié sur les rapports, vous pouvez renommer le protocole plus clairement de façon à ce que les autres utilisateurs puissent l'identifier.

Création d'une règle de mappage d'applications d'hôte

Créez une règle d'application d'hôte pour regrouper le trafic généré à partir d'un hôte. Par exemple, la règle d'application permet aux utilisateurs d'inclure facilement dans les rapports le trafic total d'un serveur ou d'une application sur le serveur.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Définitions d'application.
La page Définitions d'application s'affiche.
2. Vérifiez que Mappage d'applications est la valeur sélectionnée pour Règles.
3. Cliquez sur Ajouter une règle.
La boîte de dialogue Ajouter un mappage d'applications s'ouvre.
4. Sélectionnez Hôte dans la liste de types de règle dans la partie supérieure de la boîte de dialogue.
La boîte de dialogue Ajouter un mappage d'applications passe en mode de règle Hôte.
5. Saisissez des valeurs pour les paramètres suivants :
 - Hôte : adresse IP du serveur pour lequel vous mappez le trafic réseau.
 - Type de service : type de service à utiliser comme filtre pour les données collectées. Pour que toutes les valeurs de type de service correspondent, acceptez la valeur par défaut Tout ou laissez la zone Type de service vide.
 - Protocole : protocole des données qui seront affectées par la règle (TCP ou UDP).

- Port : port à utiliser pour la collecte de données. Pour que toutes les valeurs de port correspondent, acceptez la valeur par défaut Tout ou laissez la zone Port vide.
- Port de destination : port cible qui collectera les données mappées.
- Nom : identificateur de la règle tel qu'elle est répertoriée dans la page Définitions d'application.
- Description (facultatif) : texte descriptif complémentaire permettant d'identifier le type de règle et son utilisation.

Remarque : Si plusieurs règles de mappage d'applications ont les mêmes paramètres de destination de port et de protocole, elles portent le même nom.

6. Lorsque les valeurs sont correctes pour tous les champs requis, cliquez sur Enregistrer.

La boîte de dialogue Ajouter un mappage d'applications se ferme. La nouvelle règle est incluse dans la liste des règles de mappage d'applications.

7. (Facultatif) Lancez des rapports pour vérifier que l'ensemble du trafic sur le port cible respecte la règle.
8. (Facultatif) Une fois que vous avez constaté les effets du mappage d'applications créé ou modifié sur les rapports, vous pouvez renommer le protocole plus clairement de façon à ce que les autres utilisateurs puissent l'identifier.

Création d'une règle de mappage d'applications Tout (type de service)

La création d'une règle portant sur toutes les applications vous permet de regrouper le trafic ayant la même valeur de type de service. La règle d'application Tout permet aux utilisateurs d'inclure facilement dans les rapports le trafic total identifié correspondant à un type de service.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Définitions d'application.
La page Définitions d'application s'affiche.
2. Vérifiez que Mappage d'applications est la valeur sélectionnée pour Règles.
3. Cliquez sur Ajouter une règle.
La boîte de dialogue Ajouter un mappage d'applications s'ouvre.

4. Dans la liste de types de règle de la partie supérieure de la boîte de dialogue, sélectionnez Tout.

La boîte de dialogue Ajouter un mappage d'applications passe en mode de règle Tout (type de service).

5. Saisissez des valeurs pour les paramètres suivants :
 - Type de service : type de service à utiliser comme filtre pour les données collectées. Pour que toutes les valeurs de type de service correspondent, entrez 0.
 - Port de destination : port cible qui collectera les données mappées.
 - Nom : identificateur de la règle tel qu'elle est répertoriée dans la page Définitions d'application.
 - Description (facultatif) : texte descriptif complémentaire permettant d'identifier le type de règle et son utilisation.

6. Lorsque les valeurs sont correctes pour tous les champs requis, cliquez sur Enregistrer.

La boîte de dialogue Ajouter un mappage d'applications se ferme. La nouvelle règle est incluse dans la liste des règles de mappage d'applications.

7. (Facultatif) Lancez des rapports pour vérifier que l'ensemble du trafic sur le port cible respecte la règle.
8. (Facultatif) Examinez les effets des règles de mappage d'applications créées ou modifiées sur les rapports, puis renommez le protocole plus clairement de façon à ce que les autres utilisateurs puissent l'identifier.

Modification de règles de mappage d'applications

Modifiez une règle de mappage d'applications lorsque voulez-vous changer le port ou la plage de ports source, le port de destination, le protocole, l'hôte, le type de service, le sous-réseau, le masque, le nom de règle, la description de règle ou le type de règle.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Définitions d'application.
La page Définitions d'application s'affiche.
2. Cochez la case à côté de la règle que vous voulez modifier, puis cliquez sur Modifier.
La boîte de dialogue Modifier un mappage d'applications s'ouvre.

3. Effectuez les modifications requises, puis cliquez sur Enregistrer.
Si les modifications sont appliquées correctement, la boîte de dialogue se ferme.

Suppression de règles de mappage d'applications

Supprimez des règles de mappage d'applications lorsqu'elles sont obsolètes.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Définitions d'application.
La page Définitions d'application s'affiche.
2. Cochez la case située à côté de la règle à supprimer. Pour sélectionner les cases à cocher pour toutes les règles, cochez la case à cocher de la ligne de titre.
3. Cliquez sur Supprimer.
Un message de confirmation s'affiche.
4. Cliquez sur Oui.
La liste des règles de mappage d'applications est mise à jour pour refléter les suppressions.

Utilisation des places réservées

Vous pouvez créer des règles de places réservées pour que les rapports incluent les combinaisons de port et de protocole qui vous intéressent, indépendamment du volume ou du taux de trafic. Les règles créent des places réservées pour les ports utilisés par ces protocoles, afin de garantir que les données sont incluses dans les rapports.

Par exemple, pendant un déploiement d'application, vous voulez consulter le trafic pour une application particulière, mais les rapports N principaux protocoles pour les interfaces n'affichent pas le trafic de l'application. Le protocole utilisé par l'application n'est pas inclus dans le groupe N principaux protocoles (groupe de protocoles affichant le volume de trafic ou d'utilisation le plus élevé). Vous créez une règle Places réservées pour collecter des données pour le protocole spécifique et le port utilisé par l'application. Le protocole est désormais inclus dans les rapports N principaux protocoles.

Remarque : Les données généralement collectées par CA Network Flow Analysis sont décrites dans la rubrique [Procédure de collecte des données](#) (page 141).

Création de règles de places réservées

Créez des règles de places réservées pour que les rapports incluent les combinaisons de port et de protocole qui vous intéressent, indépendamment du volume ou du taux de trafic.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Définitions d'application.
La page Définitions d'application s'affiche.
2. Dans la liste Règles, sélectionnez Places réservées.
La page Définitions d'application bascule en mode Places réservées et affiche une liste des règles de places réservées actuelles.
3. Cliquez sur Ajouter une règle.
La boîte de dialogue Ajouter des places réservées s'ouvre.
4. Spécifiez les ports de la manière suivante :
 - Protocole : protocole des données qui seront affectées par la règle (TCP ou UDP).
 - Port : port cible pour la règle de places réservées. Introduisez le numéro de port dans la zone Port, une valeur de 0 à 65535 exprimée au format décimal de base 10. Si vous n'entrez aucune valeur, le port 0 est affecté. L'association du port et du protocole doit être unique et ne doit correspondre à aucune autre règle de places réservées.

Les données du type de protocole spécifié sont incluses dans les rapports pour ce port, indépendamment du volume ou du taux de trafic.
 - Description (facultatif) : texte d'identification pour la règle de places réservées. La description s'affiche dans la liste des règles de places réservées de la page Définitions d'application.
5. Cliquez sur Enregistrer.

Si vous avez entré une combinaison port/protocole valide et que le nombre maximum de règles n'a pas été atteint, la boîte de dialogue se ferme. La nouvelle règle s'affiche dans la liste des règles de places réservées.
6. Répétez ce processus pour chaque règle de places réservées à ajouter.

Vous pouvez spécifier un maximum de 50 règles de places réservées.

Modification de règles de places réservées

Modifiez une règle de places réservées pour appliquer des corrections au port, au protocole ou à la description spécifiée.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Définitions d'application.
La page Définitions d'application s'affiche.
2. Dans la liste Règles, sélectionnez Places réservées.
La page Définitions d'application bascule en mode Places réservées et affiche une liste des règles de places réservées actuelles.
3. Cochez la case à côté de la règle que vous voulez modifier, puis cliquez sur Modifier.
La boîte de dialogue Modifier des places réservées s'ouvre.
4. Effectuez les modifications requises pour les valeurs Protocole, Port et Description, puis cliquez sur Enregistrer.
Si les modifications sont appliquées correctement, la boîte de dialogue se ferme.

Suppression de règles de places réservées

Supprimez des règles de places réservées lorsqu'elles sont obsolètes.

Procédez comme suit :

1. Ouvrez la page Définitions d'application :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Définitions d'application.
La page Définitions d'application s'affiche.
2. Dans la liste Règles, sélectionnez Places réservées.
La page Définitions d'application bascule en mode Places réservées et affiche une liste des règles de places réservées actuelles.
3. Cochez la case située à côté de la règle à supprimer. Pour sélectionner les cases à cocher pour toutes les règles, cochez la case à cocher de la ligne de titre.

4. Cliquez sur Supprimer.
Un message de confirmation s'affiche.
5. Cliquez sur Oui.
La liste des règles de places réservées est mise à jour pour refléter les suppressions.

Utilisation des interfaces

Utilisez la page Interfaces actives pour effectuer certaines tâches sur les routeurs, les interfaces et les interfaces virtuelles personnalisées, notamment :

- [Afficher les détails](#) (page 66)
- [Rechercher un routeur, une interface ou une interface virtuelle personnalisée](#) (page 69)
- [Modifier les propriétés](#) (page 70)
- [Supprimer un routeur](#) (page 71)
- [Modifier l'affichage de la page Interfaces actives](#) (page 72)

Outre ces tâches de base, vous pouvez effectuer les tâches d'administration avancées suivantes à partir des pages Interfaces actives et Interfaces disponibles :

- [Fusion d'interfaces](#) (page 132)
- [Suppression d'une interface de la page Interfaces actives](#) (page 135)
- [Désactivation de l'affichage d'une interface dans les rapports](#) (page 135)

Fusion d'interfaces

Vous pouvez fusionner des interfaces de routeur de manière à ce qu'elles soient traitées comme un seul objet dans les rapports. Vous pouvez fusionner des interfaces pour les raisons suivantes :

- Une interface a été déplacée sur un routeur différent et vous voulez conserver les informations existantes.
- Les mises à niveau des interfaces pour un routeur génèrent un nouvel index, entraînant la création de nouvelles interfaces. Vous pouvez fusionner les anciennes interfaces avec les nouvelles.

Procédez comme suit :

1. Ouvrez la page Interfaces actives :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.
La page Interfaces actives s'ouvre et indique les routeurs actuels et leurs interfaces actives.
2. Développez la liste des interfaces d'un routeur en cliquant sur la flèche située sur la gauche de la ligne du routeur.
Une liste des interfaces pour le routeur sélectionné se développe.
3. Cochez la case située à côté des interfaces à fusionner.
Le bouton Fusionner situé dans la partie supérieure de la page est activé.
Remarque : Le bouton Fusionner est uniquement activé lorsque deux interfaces sont sélectionnées.
4. Cliquez sur Fusionner.
La boîte de dialogue Confirmation de la fusion des interfaces s'affiche.

5. Vérifiez les informations affichées dans la boîte de dialogue Confirmation de la fusion des interfaces, comme suit :
 - Assurez-vous que l'interface affichée en tant que source (définie dans les champs sous l'étiquette Emplacement des données à copier) est l'interface dont vous voulez copier les données.
 - Assurez-vous que l'interface affichée en tant que destination (définie dans les champs sous l'étiquette Emplacement des données à copier) est l'interface sur laquelle vous voulez copier les données.
 - Cochez la case Supprimer l'interface source une fois les données fusionnées pour supprimer l'interface source automatiquement après la copie des données.
6. Cliquez sur Enregistrer.

Les interfaces sélectionnées sont fusionnées selon les valeurs définies dans la boîte de dialogue Confirmation de la fusion des interfaces.

Activer les interfaces

Par défaut, les interfaces sont activées automatiquement dans CA Network Flow Analysis. Toutefois, vous devez les activer manuellement dans les cas suivants :

- Les interfaces ont été désactivées temporairement et vous voulez les réactiver.
- Le programme a été configuré de façon à ne pas activer automatiquement les nouvelles interfaces détectées. L'option Activer les interfaces automatiquement de la page Paramètres de l'application est définie sur False.

L'activation d'une interface déclenche instantanément les événements suivants :

- Les données d'examen de flux pour l'interface sont disponibles dans les rapports Examen de flux. Les données d'examen de flux que vous pouvez afficher incluent les données collectées lorsque l'interface était désactivée.
- D'autres types de données d'interface sont collectées et stockées, notamment les données relatives aux hôtes, aux conversations, aux types de service et aux prototypes. Une fois que la période initiale de collecte de données est terminée, vous pouvez afficher les données d'interface supplémentaires dans les rapports d'interface d'analyse en profondeur, dans les rapports d'analyse et dans les rapports personnalisés.

Procédez comme suit :

1. Ouvrez la page Interfaces disponibles :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Système : Activer.
La page Available Interfaces s'ouvre.
2. Cliquez sur la flèche sur la gauche de la ligne du routeur qui contient les interfaces à activer.

Une vue développée de la liste des interfaces pour le routeur sélectionné apparaît qui affiche le statut Activé.
3. Cochez la case à côté d'une ou de plusieurs interfaces.
4. Cliquez sur Activer.

Les interfaces sélectionnées sont activées immédiatement.

Suppression et désactivation des interfaces

Vous pouvez supprimer des interfaces de routeur de façon permanente lorsque les rapports individuels n'ont aucun intérêt. Par exemple, vous pouvez supprimer plusieurs interfaces LAN qui sont reliées à un routeur. Vous continuez de surveiller l'interface WAN qui transfère les données à partir du routeur. De même, vous pouvez désactiver temporairement des interfaces pour qu'elles ne soient pas inclus dans les rapports ou pour réorganiser vos rapports.

Vous pouvez supprimer et désactiver des interfaces des manières suivantes :

- *Suppression des interfaces de la page Interfaces actives* : pour supprimer une interface ou un routeur de la page Interfaces actives, suivez la procédure décrite dans la section [Suppression d'une interface de la page Interfaces actives](#) (page 135).
- *Désactivation de l'affichage des interfaces dans les rapports* : pour supprimer une interface ou un routeur des rapports CA Network Flow Analysis, mais le conserver dans la page Interfaces actives, suivez la procédure décrite dans la section [Désactivation de l'affichage d'une interface dans les rapports](#) (page 135).
- *Suppression complète d'un routeur et de ses interfaces* : pour supprimer un routeur complètement, suivez la procédure décrite dans la section [Suppression d'un routeur](#) (page 71).

Suppression d'une interface de la page Interfaces actives

Procédez comme suit :

1. Connectez-vous à la console NFA avec un compte disposant des droits d'administrateur de CA Network Flow Analysis.
2. Localisez l'interface dans la liste des interfaces surveillées et supprimez-la selon la procédure décrite dans la section [Vérification des interfaces surveillées](#) (page 34).
3. Ouvrez la page Interfaces actives :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Interfaces : physiques et virtuelles.
La page Interfaces actives s'ouvre et indique les routeurs actuels et leurs interfaces actives.
4. Développez la liste des interfaces d'un routeur en cliquant sur la flèche située sur la gauche de la ligne du routeur.
Une liste des interfaces pour le routeur sélectionné se développe.
5. Cochez la case à côté de chaque interface à supprimer.
Les boutons appropriés sont activés dans la partie supérieure de la page Interfaces actives. Les boutons Modifier et Supprimer sont activés uniquement lorsqu'une seule interface est sélectionnée.
6. Cliquez sur Supprimer.
Un message de confirmation s'affiche.
7. Cliquez sur Oui pour confirmer la suppression des interfaces sélectionnées.
Toutes les interfaces sélectionnées sont supprimées de la page Interfaces actives. En outre, les données d'historique, les interfaces virtuelles personnalisées, les cumuls et les liens associés sont supprimés. Les données d'historique supprimées incluent l'examen des flux, les rapports personnalisés, l'analyse et les interruptions.

Désactivation de l'affichage d'une interface dans les rapports

Procédez comme suit :

1. Ouvrez la page Interfaces disponibles :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Système : Activer.
La page Available Interfaces s'ouvre.

2. Développez la liste des interfaces d'un routeur en cliquant sur la flèche située sur la gauche de la ligne du routeur.

Une liste des interfaces pour le routeur sélectionné se développe.

3. Cochez la case à côté de chaque interface à désactiver.

Les boutons appropriés sont activés dans la partie supérieure de la page Interfaces disponibles. Les boutons Activer, Désactiver et Supprimer sont activés uniquement lorsqu'une seule interface est sélectionnée. Le bouton Supprimer est également activé lorsqu'un routeur entier est sélectionné.

4. Cliquez sur Désactiver.

Toutes les interfaces sélectionnées sont désactivées immédiatement et leur statut Actif est remplacé par Non. Lorsqu'elles sont désactivées, les interfaces ne s'affichent plus dans les rapports.

Modification d'adresses IP de DSA

Applicable à : une architecture à trois niveau dans un déploiement distribué (console NFA, Harvester et DSA installés sur des serveurs distincts)

Modifiez le paramètre d'adresse IP pour un DSA lorsque :

- Changement d'adresse IP pour un DSA actuel (DSA déjà en cours d'utilisation et non déplacé vers un autre serveur)
- Vous utilisez pour la première fois une DSA sur un nouveau serveur au lieu d'un DSA retiré.

Modifiez l'adresse IP de l'appliance de stockage des données retirée plutôt que d'ajouter une nouvelle instance de DSA. Sinon, les routeurs continuent d'envoyer des données au DSA retiré (et ces données n'apparaissent pas dans les rapports).

Remarques : Ces tâches s'appliquent uniquement dans les cas suivants.

- Déploiements distribué de CA Network Flow Analysis à trois niveaux. Si vous disposez d'un système autonome ou d'une architecture à deux niveaux, vous n'avez pas besoin de définir ou de mettre à jour les adresses IP de DSA.
- Serveurs Windows. CA Network Flow Analysis prend en charge les DSA sur les serveurs Windows uniquement.
- Serveurs incluant des adresses IP statiques et qui ne sont pas configurés pour utiliser le protocole DHCP (Dynamic Host Configuration Protocol).

Modification de l'adresse IP d'un DSA actuellement connecté

Modifiez le paramètre d'adresse IP du DSA en cas de modification de l'adresse IP d'un DSA actuellement connecté.

Effectuez cette tâche lorsque l'adresse IP change sur un serveur de DSA. Si vous déplacez le DSA vers un nouveau serveur, ignorez cette étape et consultez la rubrique [Modification de l'adresse IP d'un nouveau DSA](#) (page 138).

Procédez comme suit :

1. Connectez-vous avec un compte disposant des droits d'administrateur de CA Network Flow Analysis.
2. Interrompez la collecte de données du DSA actuel :
 - a. Ouvrez la fenêtre Services Windows sur le serveur de DSA.
 - b. Sélectionnez le service de pompage de NetQoS Reporter Analyzer dans la liste Services.
 - c. Cliquez sur le lien Arrêter à gauche.
L'exécution du service s'arrête.
3. Attendez que le DSA termine le traitement des fichiers .rpr dans le répertoire suivant : <chemin_installation>/Netflow/datafiles/loaderInput.

Cette étape permet au DSA de récupérer les données brutes qui ont été générées lors de l'arrêt du service. Le traitement prend environ 15 minutes. Le traitement se termine lorsqu'il ne reste plus de fichiers .rpr dans le répertoire loaderInput.
4. Changez l'adresse IP sur le serveur de DSA. Pour plus d'informations sur cette étape, consultez les recommandations sur le site microsoft.com.
5. Mettez à jour les paramètres de pare-feu si nécessaire.
6. Affichez la page DSA dans l'interface utilisateur de la console NFA :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Système : DSA.
La page DSA s'ouvre et affiche la liste des DSA utilisés.
7. Dans la ligne du DSA que vous souhaitez modifier, cliquez sur Modifier.
La boîte de dialogue Modifier le DSA s'affiche.
8. Remplacez la valeur du champ Adresse IP par l'adresse IP du nouveau serveur de DSA.
9. Cliquez sur Tester la connexion.
Si la connexion réussit, le message Test réussi s'affiche.

10. Cliquez sur OK dans la zone de message Test réussi.
Le message se ferme.
11. Cliquez sur Enregistrer dans la boîte de dialogue Modifier le DSA.
La nouvelle adresse IP du DSA est enregistrée. CA Network Flow Analysis commence à utiliser la nouvelle adresse IP dès qu'il commence à stocker et à récupérer des données.
12. Redémarrez le service de pompage de NetQoS Reporter Analyzer dans la fenêtre Services Windows sur le serveur de DSA.
Le DSA commence de nouveau à collecter des données. Il doit pouvoir récupérer toutes les données générées pendant la période d'arrêt du service.

Modification de l'adresse IP d'un nouveau DSA

Modifiez l'adresse IP du DSA pour commencer à utiliser un nouveau DSA au lieu du DSA retirée.

Effectuez cette tâche pour déplacer le DSA vers un nouveau serveur. Par exemple, en cas d'échec du serveur de DSA ou pour améliorer les performances ou l'espace de stockage. Une fois que vous remplacez l'adresse IP par l'adresse du nouveau serveur, la permutation vers le nouveau DSA est terminée.

Remarques :

- Si vous déplacez un DSA vers un nouveau serveur, les données du DSA antérieur ne sont plus disponibles dans les rapports.
- Si vous ajoutez une instance de DSA au lieu de modifier l'adresse IP d'un DSA retiré, le DSA retiré apparaît encore dans la liste. Les routeurs répartissent les données entre tous les DSA de la liste, c'est pourquoi les routeurs continuent d'envoyer des données au DSA retiré. Les rapports n'incluent pas les données qui sont envoyées vers des DSA non fonctionnels. Pour corriger ce problème, contactez le service de support de CA pour obtenir de l'aide pour la suppression du DSA obsolète.
- Si le DSA se trouve toujours sur le même serveur, ignorez cette tâche et consultez la rubrique [Modification de l'adresse IP d'un DSA actuellement connecté](#) (page 137).

Procédez comme suit :

1. Installez le logiciel de DSA sur le nouveau serveur et terminez la configuration (y compris les mises à jour de pare-feu). Pour plus d'informations sur cette étape, consultez le *Manuel d'installation de CA Network Flow Analysis 9.1.3*.
2. Connectez-vous à la console NFA avec un compte disposant des droits d'administrateur de CA Network Flow Analysis.
3. Exécutez et enregistrez les copies des rapports que vous voulez utiliser pour les informations d'archivage du DSA précédent.

4. Affichez la page DSA dans l'interface utilisateur de la console NFA :
 - a. Dans le menu de console NFA, sélectionnez Administration.
La page Administration s'ouvre.
 - b. Dans le menu Administration, sélectionnez Système : DSA.
La page DSA s'ouvre et affiche la liste des DSA utilisés.
5. Dans la ligne du DSA que vous allez remplacer, cliquez sur Modifier.
La boîte de dialogue Modifier le DSA s'affiche.
6. Remplacez la valeur du champ Adresse IP par l'adresse IP du nouveau serveur de DSA.
7. Cliquez sur Tester la connexion.
Si la connexion réussit, le message Test réussi s'affiche.
8. Cliquez sur OK dans la zone de message Test réussi.
Le message se ferme.
9. Cliquez sur Enregistrer dans la boîte de dialogue Modifier le DSA.
La nouvelle adresse IP du DSA est enregistrée. Le nouveau DSA commence à collecter, à traiter et à stocker les données. Les données du DSA retiré ne sont plus disponibles dans les rapports.

Chapitre 7: Analyse et maintenance des données collectées

Grâce aux données qu'il collecte, CA Network Flow Analysis est un outil performant d'analyse du trafic réseau. Les rubriques suivantes fournissent des informations sur les données collectées, les bases de données utilisées pour les stocker, ainsi que sur la sauvegarde et la restauration de ces bases de données.

Ce chapitre traite des sujets suivants :

[Collecte de données](#) (page 141)

[Sauvegarde et restauration des données de CA Network Flow Analysis](#) (page 148)

[Recommandations liées à la préservation de l'intégrité des données](#) (page 158)

Collecte de données

La version 9.1.00 de CA Network Flow Analysis et les versions ultérieures prennent en charge une architecture à deux niveaux. CA Network Flow Analysis 9.1.3 prend également en charge les mises à niveau de déploiements de CA NetQoS ReporterAnalyzer 9.0.161 pour des architectures à trois niveaux. Dans les deux architectures, les composants fonctionnent ensemble pour collecter, traiter et stocker les données de flux. Affichez les données dans des rapports et générez les interruptions, les événements et les rapports planifiés.

L'architecture à deux niveaux comprend la console NFA et au moins une instance du nouveau Harvester (combinaison du Harvester antérieur et du composant DSA). L'empreinte du déploiement est réduite et le nombre de types de composants requérant une mise à niveau et une maintenance est réduit. En plus, la gestion des données requiert moins d'étapes et la fréquence d'envoi des fichiers est réduite.

Le déploiement d'architecture à trois niveaux comprend la console NFA, au moins un Harvester et au moins un DSA. Si vous mettez à niveau à partir d'un déploiement distribué de CA NetQoS ReporterAnalyzer 9.0.161, vous continuerez d'utiliser l'architecture à trois niveaux. L'architecture à trois niveaux convient mieux pour un environnement comprenant des serveurs de DSA avec une latence plus faible que celle des serveurs du Harvester. L'architecture à trois niveaux place également les demandes de stockage plus légères sur les serveurs du Harvester.

Procédure de collecte des données dans un déploiement à 2 niveaux

La console NFA et le Harvester fonctionnent ensemble de la façon suivante dans un déploiement d'architecture à 2 niveaux :

Nouveau Harvester

Il extrait les flux bruts des routeurs, analyse les données et compile les données historiques (15 minutes) et les données de résolution en 1 minute. Le Harvester stocke les données suivantes :

- Données de flux bruts
- Données de résolution en 1 minute
- Données historiques (15 minutes)

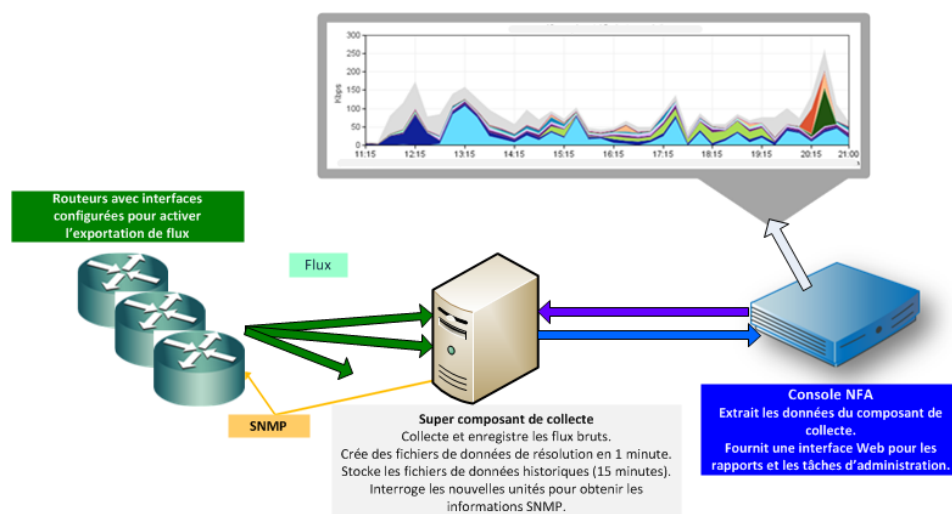
Remarque : Il est important que le serveur du Harvester dispose d'assez d'espace de stockage, car il stocke davantage de types de données que dans un déploiement d'architecture à trois niveaux.

Console NFA

Elle collecte les données à partir du Harvester et affiche les données de rapport dans l'interface Web. Elle stocke les données de présentation de l'entreprise.

Elle fournit une interface utilisateur Web pour les tâches administratives et signale et stocke les données de présentation de l'entreprise. Les rapports contiennent les données suivantes :

- Données de présentation de l'entreprise stockées localement
- Données de résolution en 1 minute et 15 minutes et données stockées sur le Harvester



Procédure de collecte des données dans un déploiement à 3 niveaux

La composants de console NFA, Harvester et DSA fonctionnent ensemble de la façon suivante dans un déploiement d'architecture à trois niveaux :

Harvester

Il extrait les flux bruts des routeurs, analyse les données et les enregistre.

Il stocke les données de résolution en 1 minute données et les données de flux bruts. Les données de flux bruts des dernières 24 heures sont stockées.

Console NFA

Elle rassemble les données de présentation de l'entreprise et les données de résolution en 15 minutes (historique) à partir du Harvester et agrège les données de résolution en 15 minutes.

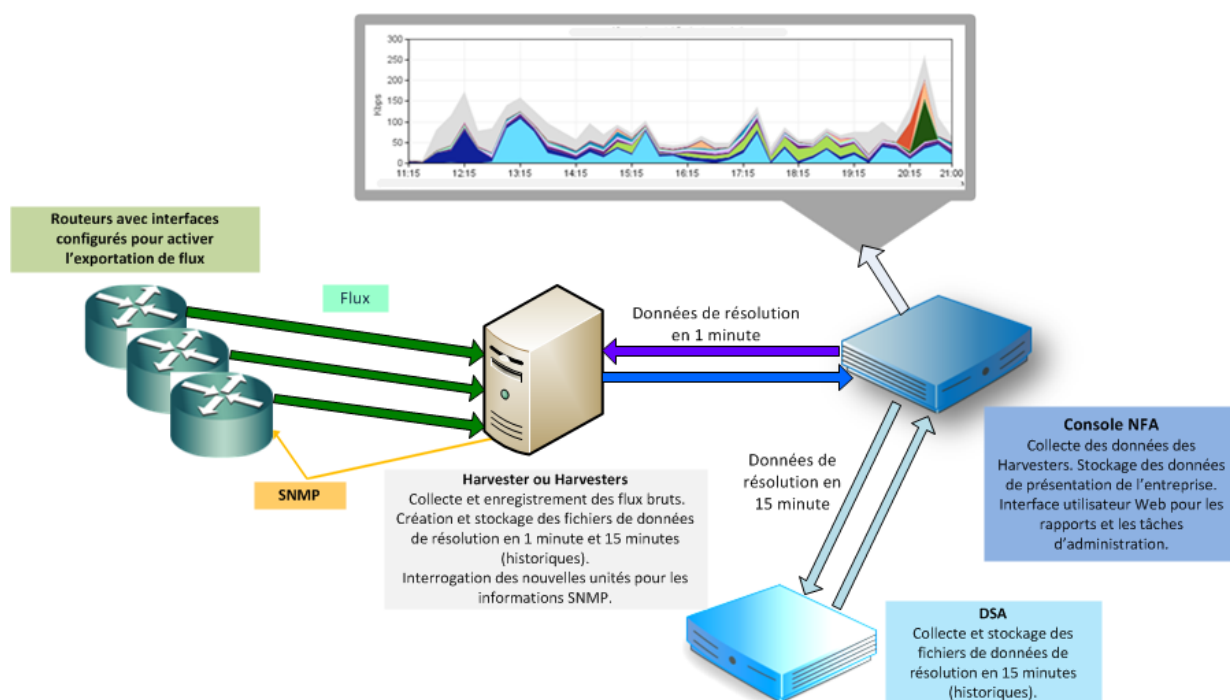
Elle stocke les données de présentation de l'entreprise.

Elle fournit une interface utilisateur Web pour les tâches d'administration et les rapports. Les rapports contiennent les données suivantes :

- Données de présentation de l'entreprise stockées localement
- Données de résolution en 1 minute stockées sur le Harvester
- Données de résolution en 15 minutes stockées sur le DSA

DSA

Il collecte les données de résolution en 15 minutes (historique) à partir de la console NFA et les stocke.



Données de la présentation de l'entreprise

Les données de présentation de l'entreprise sont collectées et affichées dans la page Présentation de l'entreprise. Pour chaque rapport, un maximum de 12 interfaces, protocoles ou hôtes est inclus pour toute l'entreprise. Les vues de présentation de l'entreprise se basent sur les 24 dernières heures de la collecte de données. Les données sont affichées dans les rapports suivants :

- Utilisation de l'interface
Sélection : seuils définis par l'utilisateur pour l'utilisation de la capacité des interfaces.
- Principales interfaces - En entrée (trafic entrant) et Principales interfaces - En sortie (trafic sortant)
Sélection : taux de capacité d'interface utilisée pendant la période de rapport. Le calcul de l'utilisation se base sur le volume de données et la vitesse des interfaces. La vitesse des interfaces dérive de l'interrogation SNMP.

- Principaux protocoles

Sélectionné : volume de trafic utilisant les protocoles.

- Principales interfaces pour le protocole

Sélection : volume de trafic d'interfaces pour le protocole sélectionné dans la vue Principaux protocoles.

- Principaux hôtes pour le protocole

Sélection : volume de trafic d'hôtes pour le protocole sélectionné dans la vue Principaux protocoles.

- Principaux hôtes

Sélection : volume de trafic total généré par les hôtes.

- Principales interfaces pour l'hôte

Sélection : volume de trafic d'interfaces pour l'hôte sélectionné dans la vue Principaux hôtes.

- Principaux protocoles pour l'hôte

Sélection : volume de trafic de protocoles pour l'hôte sélectionné dans la vue Principaux hôtes.

Durée de vie des données : les données de présentation de l'entreprise sont conservées pendant 1 mois par défaut.

Emplacement de stockage : les données sont stockées dans la console NFA dans les déploiements à deux niveaux et à trois niveaux.

Données de résolution en 15 minutes

Les types de données suivants sont collectés et stockés en tant que données de résolution en 15 minutes par défaut.

Trafic global

- Total du trafic IP, TCP et UDP entrant et sortant de chaque interface
- Flux et octets du flux de trafic entrant et sortant de chaque interface
- Total du flux de trafic de chaque routeur

Les données d'intervalle de 15 minutes reflètent les totaux pour chaque interface, mais les données de présentation de l'entreprise reflètent les totaux pour toutes les interfaces. Par exemple, les données de présentation de l'entreprise incluent les N principaux protocoles pour toutes les interfaces. Les données d'intervalle de 15 minutes incluent les N principaux protocoles pour chaque interface.

Hôtes

Le trafic sortant et entrant des 50 principaux hôtes IP

Conversations

Trafic des 50 principales conversations IP

Protocoles

- *Global* : 100 principaux protocoles entrants et sortants de chaque interface
Les règles de places réservées vous permettent d'inclure des protocoles spécifiques dans le groupe des principaux protocoles indépendamment de leur volume de trafic.
- *Protocoles - Hôtes* : trafic sortant et entrant des 10 principaux hôtes pour les 20 principaux protocoles
- *Protocoles - Conversations* : trafic des 10 principales conversations pour les 20 principaux protocoles

Type de service

- *Global* : total du trafic IP entrant et sortant de chaque interface pour chaque valeur de type de service
- *Type de service - Protocoles* : trafic des 20 principaux protocoles pour les 5 principales valeurs de type de service non nulles
- *Type de service - Hôtes* : trafic des 10 principaux hôtes pour les 5 principales valeurs de type de service non nulles
- *Type de service - Conversations* : trafic des 10 principales conversations pour les 5 principales valeurs de type de service non nulles

Système autonome

- 100 principales sources et destinations des valeurs de système autonome
- 20 principales adresses de tronçon suivant pour chaque valeur de système autonome

Le trafic de système autonome est stocké pendant 100 jours par défaut.

Durée de vie des données : chaque type de données inclut une période de stockage maximum par défaut, comme l'illustre la liste suivante :

- Trafic global : 372 jours ou 12,4 mois
- Protocoles (100 principaux) : 372 jours ou 12,4 mois
- Hôtes, Protocoles - Hôtes et Type de service - Hôtes : 67 jours
- Conversations (50 principaux), Protocoles - Conversations et Type de service - Conversations : 67 jours
- Type de service et Type de service - Protocoles : 372 jours ou 12,4 mois
- Système autonome : 100 jours

Seuils minimum : pour être inclus dans un rapport de données de résolution en 15 minutes, le trafic de données doit correspondre aux seuils minimum par défaut ou dépasser la période de 15 minutes :

- Protocoles : 50 Ko
- Hôtes : 100 Ko
- Conversations : 100 Ko
- Type de service : Aucun minimum
- Système autonome : Aucun minimum

Emplacement de stockage : les données historiques (15 minutes) sont stockées sur le nouveau Harvester dans un déploiement à deux niveaux et sur le DSA dans un déploiement à trois niveaux.

Rapports : les données de résolution en 15 minutes sont souvent utilisées pour examiner les tendances et effectuer une analyse de la capacité. Elles apparaissent dans les rapports suivants :

- Rapports d'interfaces configurés pour indiquer des plages horaires de plus de 2 heures
- Rapports personnalisés
- Rapports d'analyse
- Vues et rapports CA Performance Center de données CA Network Flow Analysis configurés pour afficher des plages horaires de plus de 2 heures

Données de résolution en 1 minute

Les types de données suivants sont stockés en tant que données de résolution en 1 minute par défaut.

Hôtes

Trafic sortant et entrant des 300 principaux hôtes IP

Conversations

Trafic sortant et entrant des 300 principales conversations IP

Protocoles

- *Global* : 150 principaux protocoles pour le trafic entrant et sortant de chaque interface
- *Hôtes* : trafic sortant et entrant des 25 principaux hôtes utilisant les 25 principaux protocoles
- *Conversations* : trafic des 25 principales conversations utilisant les 25 principaux protocoles

Type de service

- *Protocoles* : trafic des 25 principaux protocoles pour les 5 principales valeurs de types de services
- *Hôtes* : trafic des 25 principaux hôtes pour les 5 principales valeurs de types de services
- *Conversations* : trafic des 25 principales conversations pour les 5 principales valeurs de types de services

Durée de vie des données : la période de stockage maximum par défaut des données de résolution en 1 minute est de 1 mois.

Emplacement de stockage : les données de résolution en 1 minute sont stockées dans le Harvester dans les déploiements à deux niveaux et à trois niveaux.

Rapports : ce type de données est souvent utilisé pour le dépannage et une analyse précise. Les données s'affichent dans les rapports suivants, lorsque les rapports sont configurés pour afficher des plages horaires d'un maximum de 2 heures :

- Vues d'interface et rapports
- Vues CA Performance Center et rapports de données CA Network Flow Analysis

Données brutes : les données brutes sont utilisées pour une analyse plus détaillée dans des rapports d'examen des flux. Les données brutes sont stockées sur le Harvester pour un maximum de 24 heures par défaut.

Sauvegarde et restauration des données de CA Network Flow Analysis

Effectuez les opérations décrites dans cette section pour sauvegarder et restaurer les bases de données de CA Network Flow Analysis. Vous pouvez sauvegarder des bases de données CA Network Flow Analysis manuellement (suivez les instructions incluses dans cette section) ou sauvegarder les bases de données automatiquement. Pour sauvegarder les bases de données automatiquement, ajoutez les répertoires appropriés à votre routine de sauvegarde régulière, par exemple :

- Fichiers de configuration personnalisés : emplacements personnalisés (tout serveur)
- Base de données personnalisée du service de conservation des données :
<chemin_installation>\MySQL51\data\data_retention (serveurs de Harvester ou autonomes)
- Données de présentation de l'entreprise et données de configuration de la console NFA : <chemin_installation>\MySQL51\data\reporter (serveur de console NFA)

- Données historiques (15 minutes) sur un serveur autonome ou un déploiement distribué à deux niveaux :
<chemin_installation>\Netflow\datafiles\ReaperArchive15 (serveur de Harvester ou autonome)
- Données historiques (15 minutes) sur un déploiement distribué à trois niveaux :
<chemin_installation>\MySQL51\data\nqrptr (serveur de DSA)
- Données de configuration du Harvester : <chemin d'installation de NFA>\mysql51\data\harvester (serveur de Harvester ou autonome)
- Données d'interrogateur : <chemin_installation>\mysql51\data\poller (serveur de Harvester ou autonome).

Important :

- Exécutez les sauvegardes simultanément. Des problèmes peuvent en résulter si vous restaurez des données à partir de sauvegardes dont les horodatages sont différents. Vérifiez que vos fichiers de données sauvegardés indiquent la même heure.
- Stockez les sauvegardes à un emplacement distant pour pouvoir les récupérer en cas de panne de matériel ou de système d'exploitation sur le serveur principal. Par exemple, sauvegardez les bases de données sur un partage administratif ou un lecteur réseau mappé.

Tenez compte des [remarques générales relatives à la fréquence de sauvegarde](#) (page 150).

Avant de sauvegarder des bases de données volumineuses, tenez compte de la quantité d'espace disque requis pour les sauvegardes et de la durée de vie des fichiers que vous sauvegardez. Les données de flux brutes (fichiers NFA) ou le répertoire de fichiers de données complet ne doivent pas être nécessairement être inclus dans la sauvegarde.

Bases de données à sauvegarder

CA Network Flow Analysis utilise plusieurs bases de données pour stocker des données de configuration, des données de résolution en 15 minutes (historiques), des données de résolution élevée (1 minute) et des données de présentation de l'entreprise. Cette rubrique décrit les bases de données à inclure dans les sauvegardes et fournit des recommandations générales relatives à la fréquence de sauvegarde. Les données sont utilisées différemment dans des environnements différents, c'est pourquoi vos priorités de sauvegarde pour prévenir la perte de données peuvent varier.

All Servers (Tous les serveurs)

- Fichiers de configuration personnalisés : sauvegardez les autres fichiers de configuration personnalisés (fichiers personnalisés par vous ou par le service de support de CA).

Emplacement : fichiers .config, .conf ou .ini localisés n'importe où à l'emplacement d'installation de CA Network Flow Analysis

Recommandation : sauvegarde quotidienne

Programme d'authentification unique (CA Performance Center)

Sauvegardez tout paramètre de configuration d'authentification unique personnalisé sur le serveur de CA Performance Center indépendamment du type de déploiement CA Network Flow Analysis. Si vous perdez des paramètres d'authentification unique personnalisés, il se peut que vous ne puissiez plus vous connecter à CA Performance Center et à CA Network Flow Analysis.

- Fichiers de configuration d'authentification unique, décrits dans la rubrique Fichiers de configuration d'authentification unique du *Manuel d'installation de CA Performance Center*.

Console NFA (déploiement distribué)

- Base de données du générateur de rapports : le contenu inclut les 24 dernières heures de données de présentation de l'entreprise, les paramètres et les informations de synchronisation.

Emplacement : <chemin_installation>\mysql51\data\reporter

Recommandation : sauvegarde hebdomadaire

Harvester (déploiement distribué)

- Données historiques (15 minutes) (base de données ReaperArchive15 dans un déploiement distribué à deux niveaux) : le contenu de cette base de données inclut les données de résolution en 15 minutes stockées pour les routeurs de génération de rapports et les interfaces.

Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive15

Recommandation : sauvegarde hebdomadaire

- Fichiers de configuration du Harvester et de l'interrogateur : les données de configuration de l'interrogateur et du Harvester sont essentielles pour effectuer le mappage relationnel qui fournit l'accès aux données de résolution en 15 minutes. Les données de configuration de l'interrogateur fournissent des informations concernant les unités et les interfaces pour activer l'interrogation, telles que les ID persistants pour les interfaces.

Emplacements : <chemin_installation>\MySQL51\data\harvester et
<chemin_installation>\MySQL51\data\poller

Recommandation : sauvegarde quotidienne

- (Facultatif) Données d'examen des flux (base de données HarvesterArchive) :

Emplacement : <chemin_installation>\Netflow\datafiles\HarvesterArchive

De nombreux administrateurs ne sauvegardent pas les données d'examen des flux, car leur durée de stockage est courte (maximum de 24 heures).

- (Facultatif) Fichiers de données à haute résolution (1 minute) (base de données ReaperArchive) : de nombreux administrateurs ne sauvegardent pas les données de résolution en 1 minute, car leur volume élevé requiert de longues sauvegardes. Lorsque vous décidez de sauvegarder ces fichiers, tenez compte des facteurs :
 - Valeur de ces données calculée sur une base quotidienne
 - Durée de sauvegarde élevée

Les données de résolution en 1 minute sont stockées pendant un mois.

Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive

- Fichiers de configuration de conservation des données personnalisées : si vous avez personnalisé des paramètres de conservation de données, sauvegardez les données de configuration de conservation de données.

Remarque : Les paramètres de conservation de données ne sont généralement pas personnalisés, sauf avec l'aide du support CA. Les modifications apportées aux paramètres de conservation des données peuvent créer des problèmes, lorsque l'espace du lecteur utilisé augmente.

Emplacement : <chemin_installation>\MySQL51\data\data_retention

Recommandation : sauvegarde quotidienne

DSA (déploiement distribué à trois niveaux)

- Données historiques (15 minutes) (base de données ReaperArchive15 dans un déploiement distribué à trois niveaux) : le contenu de cette base de données inclut les données de résolution en 15 minutes stockées pour les routeurs de génération de rapports et les interfaces.

Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive15

Recommandation : sauvegarde hebdomadaire

- Données historiques (15 minutes) (base de données MySQL nqrptr) : ce répertoire contient les paramètres de DSA.

Emplacement : <chemin_installation>\MySQL51\data\nqrptr

Recommandation : sauvegarde hebdomadaire

Serveur autonome

- Base de données de générateur de rapports : le contenu de cette base de données inclut les données de présentation de l'entreprise, les paramètres et les informations de synchronisation pour les 24 dernières heures.

Emplacement : <chemin_installation>\mysql51\data\reporter

Recommandation : sauvegarde hebdomadaire

- Données historiques (15 minutes) (base de données ReaperArchive15) : le contenu de cette base de données inclut les données de résolution en 15 minutes stockées pour les routeurs de génération de rapports et les interfaces.

Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive15

Recommandation : sauvegarde hebdomadaire

- Fichiers de configuration du Harvester et de l'interrogateur : les données de configuration de l'interrogateur et du Harvester sont essentielles pour effectuer le mappage relationnel qui fournit l'accès aux données de résolution en 15 minutes. Les données de configuration de l'interrogateur fournissent des informations concernant les unités et les interfaces pour activer l'interrogation, telles que les ID persistants pour les interfaces.

Emplacements : <chemin_installation>\MySQL51\data\harvester et

<chemin_installation>\MySQL51\data\poller

Recommandation : sauvegarde quotidienne

- (Facultatif) Données d'examen des flux (base de données HarvesterArchive) :

Emplacement : <chemin_installation>\Netflow\datafiles\HarvesterArchive

De nombreux administrateurs ne sauvegardent pas les données d'examen des flux, car leur durée de stockage est courte (maximum de 24 heures par défaut).

- (Facultatif) Fichiers de données à haute résolution (1 minute) (base de données ReaperArchive) : de nombreux administrateurs ne sauvegardent pas les données de résolution en 1 minute, car leur volume élevé requiert de longues sauvegardes. Lorsque vous décidez de sauvegarder ces fichiers, tenez compte des facteurs :

- Valeur de ces données calculée sur une base quotidienne
- Durée de sauvegarde élevée

Les données de résolution en 1 minute sont stockées par défaut pendant un mois.

Emplacement : <chemin_installation>\Netflow\datafiles\ReaperArchive

- Fichiers de configuration de conservation des données personnalisées : si vous avez personnalisé des paramètres de conservation de données, sauvegardez les données de configuration de conservation de données.

Remarque : Les paramètres de conservation de données ne sont généralement pas personnalisés, sauf avec l'aide du support CA. Les modifications apportées aux paramètres de conservation des données peuvent créer des problèmes, lorsque l'espace du lecteur utilisé augmente.

Emplacement : <chemin_installation>\MySQL51\data\data_retention

Recommandation : sauvegarde quotidienne

Arrêt des services

Pour préparer la sauvegarde de bases de données, arrêtez les services sur tous les serveurs Windows dans le déploiement de CA Network Flow Analysis.

Procédez comme suit :

1. Ouvrez la fenêtre Services : cliquez sur Démarrer, Panneau de configuration, Outils d'administration, Services.
2. Arrêtez le service de Harvester (service de Harvester NetQoS ou Harvester CA NFA) sur chaque serveur.
3. Patientez 15 minutes jusqu'à la fin du traitement des fichiers de données.
4. Arrêtez les services CA Network Flow Analysis sur chaque serveur :

Service	Autonome	Harvester	Console	DSA
Services Web de collecte et d'interrogation de CA NFA (Linux : nfa_collpollws)	Oui	Oui		
Conservation de données CA NFA (Linux : nfa_dataretention)	Oui	Oui		Oui
Proxys DNS/SNMP CA NFA (Linux : nfa_proxies)	Oui	Oui	Oui	Oui
CA NFA DSALoader				Oui
Serveur de fichiers CA NFA (Linux : nfa_filewebservice)	Oui	Oui	Oui (3 niveaux)	
Harvester CA NFA (Linux : nfa_harvester)	Oui	Oui		
Interrogateur CA NFA (Linux : nfa_poller)	Oui	Oui		
Service de pompage CA NFA				Oui
Reaper CA NFA (Linux : nfa_reaper)		Oui		

Service	Autonome	Harvester	Console	DSA
Source de la base d'informations de génération de rapports de CA NFA	Oui		Oui	
NetQoS MySQL51 (Linux : mysql51)	Oui	Oui	Oui	Oui
NetQoS NQMySQL51 (Linux : nfa_mysqlCSE)	Oui	Oui	Oui	Oui
Service de gestionnaire de NetQoS Reporter	Oui		Oui	
Services généraux de NetQoS Reporter/Analyzer	Oui		Oui	
Service de pompage de NetQoS Reporter/Analyzer	Oui		Oui	
Services de requête NetQoS Reporter/Analyzer	Oui		Oui	
Service de rapport de NetQoS Reporter/Analyzer	Oui		Oui	
Outil de surveillance de NetQoS Reporter/Analyzer	Oui		Oui	

Les services et la collecte de données s'arrêtent. Les fichiers de données sont traités en 15 minutes.

5. Vérifiez le répertoire suivant sur le serveur de la console NFA :

<chemin d'installation de NFA>\Netflow\datafiles\HarvesterWork

Si le répertoire HarvesterWork est vide, [sauvegardez les bases de données](#) (page 155).

Sauvegarde des bases de données

Avant d'effectuer des sauvegardes, arrêtez les services sur les serveurs de composant CA Network Flow Analysis et vérifiez que les répertoires HarvesterWork sont vides.

Important :

- Exécutez les sauvegardes simultanément. Des problèmes peuvent en résulter si vous restaurez des données à partir de sauvegardes dont les horodatages sont différents. Vérifiez que vos fichiers de données sauvegardés indiquent la même heure.
- Stockez les sauvegardes à un emplacement distant pour pouvoir les récupérer en cas de panne de matériel ou de système d'exploitation sur le serveur principal. Par exemple, sauvegardez les bases de données sur un partage administratif ou un lecteur réseau mappé.

Procédez comme suit :

1. Identifiez les bases de données CA Network Flow Analysis et les fichiers à sauvegarder.

Les bases de données CA Network Flow Analysis et les fichiers à sauvegarder sont répertoriés dans le tableau suivant et décrits dans la rubrique [Bases de données à sauvegarder](#) (page 150).

Base de données	Serveur autonome	Serveurs de Harvester (distribués)	Serveur de console NFA (distribué)	DSA (distribué à 3 niveaux)
reporter	Important		Important	
harvester	Important	Important		
poller	Important	Important		
ReaperArchive15	Recommandé	Recommandé		Recommandé
Fichiers personnalisés	Important	Important	Important	Important
data_retention personnalisée	Important si personnalisé	Important si personnalisé		Important si personnalisé
HarvesterArchive	Facultatif, rarement sauvegardé	Facultatif, rarement sauvegardé		
ReaperArchive	Facultatif, rarement sauvegardé	Facultatif, rarement sauvegardé		
nqrptr				Important

Base de données	Serveur autonome	Serveurs de Harvester (distribués)	Serveur de console NFA (distribué)	DSA (distribué à 3 niveaux)
Registre Windows	Important	Important (Windows)	Important	Important

2. Copiez chaque fichier ou répertoire cible dans un emplacement distant.

La liste suivante indique les emplacements de bases de données :

- Fichiers de configuration personnalisés : divers emplacements
- Base de données data_retention personnalisée : <chemin d'installation de NFA>\MySQL51\data\data_retention
- Base de données harvester : <chemin_installation>\MySQL51\data\harvester
- Base de données HarvesterArchive :
<chemin_installation>\Netflow\datafiles\HarvesterArchive
- Base de données nqrptr : <chemin_installation>\MySQL51\data\nqrptr
- Base de données poller : <chemin_installation>\MySQL51\data\poller
- Base de données ReaperArchive :
<chemin_installation>\Netflow\datafiles\ReaperArchive
- Base de données ReaperArchive15 :
<chemin_installation>\Netflow\datafiles\ReaperArchive15
- Base de données reporter : <chemin_installation>\MySQL51\data\reporter
- Registre Windows :
Sauvegardez le registre sous forme de fichier .reg en sélectionnant Fichier, Exporter dans la fenêtre Editeur de registre. Pour plus d'informations sur le nouvel emplacement des paramètres du Harvester, consultez la rubrique Déplacement des paramètres du Harvester dans les Notes de parution.
- Fichiers de configuration d'authentification unique : sauvegardez les fichiers et les répertoires suivants sur le serveur d'authentification unique, qui peut être le serveur de CA Performance Center.
 - Fichier <chemin_installation>\Portal\SSO\start.ini
 - Répertoire <chemin_installation>\Portal\SSO\etc
 - Fichier <chemin_installation>\Portal\SSO\conf\wrapper.conf
 - Répertoire <chemin_installation>\Portal\SSO\webapps\sso\configuration

3. Redémarrez le service NetQoS Mysql51 et les services CA Network Flow Analysis dépendants :
 - a. Cliquez avec le bouton droit de la souris sur le service NetQoS Mysql51 dans la fenêtre Services, puis cliquez sur Redémarrer.
Le message de confirmation Restart Other Services (Redémarrer d'autres services) s'ouvre et répertorie tous les services CA Network Flow Analysis dépendants qui redémarreront également.
 - b. Cliquez sur Oui.
 - c. Le message de confirmation se ferme et les services s'arrêtent et redémarrent.
4. Redémarrez les [services](#) (page 153) de CA Network Flow Analysis.

Restauration des bases de données

Vous pouvez restaurer les données à partir d'une sauvegarde de base de données CA Network Flow Analysis. La procédure décrite dans cette rubrique a pour but de restaurer les données sur un serveur Windows, mais le chemin d'accès à la base de données est le même pour un serveur Linux.

Procédez comme suit :

1. Connectez-vous avec des droits d'administrateur.
2. [Arrêtez les services de CA Network Flow Analysis](#) (page 153).
3. Restaurez chaque fichier ou répertoire cible depuis son emplacement distant vers son emplacement d'origine :
 - Fichiers de configuration personnalisés : divers emplacements (tout serveur)
 - Base de données personnalisée du service de conservation des données : <chemin_installation>\MySQL51\data\data_retention (serveur de Harvester ou autonome)
 - Base de données harvester : <chemin_installation>\MySQL51\data\harvester (serveur de Harvester ou autonome)
 - Base de données nqrptr : <chemin_installation>\MySQL51\data\nqrptr (serveur de DSA)
 - Base de données poller : <chemin_installation>\MySQL51\data\poller (serveur autonome ou de Harvester)
 - Base de données HarvesterArchive : <chemin_installation>\Netflow\datafiles\HarvesterArchive (serveur autonome ou de Harvester)
 - Base de données ReaperArchive : <chemin_installation>\Netflow\datafiles\ReaperArchive (serveur autonome ou de Harvester)

- Base de données ReaperArchive15 :
<chemin_installation>\Netflow\datafiles\ReaperArchive15 (serveur autonome ou de Harvester)
 - Base de données reporter : <chemin_installation>\MySQL51\data\reporter (serveur autonome, de console NFA ou de DSA)
1. Redémarrez les services CA Network Flow Analysis qui sont répertoriés dans la rubrique [Arrêt des services](#) (page 153).

Recommandations liées à la préservation de l'intégrité des données

Pour garantir l'intégrité des données et empêcher l'endommagement des bases de données CA Network Flow Analysis, implémentez les recommandations suivantes sur les serveurs ou les systèmes matériels utilisés pour l'exécution des composants CA Network Flow Analysis :

- Excluez les répertoires suivants des analyses d'antivirus en temps réel :
C:\Windows\Temp et <chemin_installation_NFA>, ainsi que tous ses sous-répertoires.
- N'implémentez pas la compression de l'espace disque.
- N'installez aucun logiciel tiers, sauf les types de logiciel suivants : antivirus, gestionnaire de système et synchronisateur horaire.
- Installez les mises à jours critiques de Microsoft. Utilisez votre meilleur jugement pour décider d'installer des mises à jour facultatives.
- Défragmentez l'unité de disque le moins souvent possible. Une défragmentation fréquente n'est pas nécessaire ; les composants CA Network Flow Analysis écrivent généralement de façon séquentielle dans les bases de données et la fragmentation de données en est ainsi réduite.

Glossaire

15 minutes, données d'historique

Les données d'intervalle de 15 minutes (historique) sont des informations qui sont collectées pour chaque interface sur une plus longue période. Les informations incluent les protocoles, les hôtes et les conversations pour chaque interface. Les données récapitulatives sont également collectées pour le type de service, les principaux protocoles pour les principales valeurs de type de service et les principaux hôtes et conversations pour les principales valeurs de type de service. Les données sont stockées dans une base de données MySQL nommée `nqrptr`, située à l'emplacement `<chemin_installation_NFA>\MySQL51\data\nqrptr`.

Administrateur

Un *administrateur*, dans le contexte de ce document, est une personne qui est responsable de l'administration de CA Network Flow Analysis dans la console NFA. Un administrateur gère également les éléments dans la console CA Performance Center qui sont associés à CA Network Flow Analysis, comme les profils SNMP, les domaines IP, les groupes, les comptes d'utilisateurs, les autorisations, les droits et les rôles.

Authentification unique

L'*authentification unique* est le schéma d'authentification utilisé par CA Network Flow Analysis et par les autres sources de données CA prises en charge par CA Performance Center. Le composant d'authentification unique fournit la page de connexion qui prend en charge l'authentification des utilisateurs dans CA Performance Center et dans les produits de source de données. Une fois que les utilisateurs sont authentifiés dans CA Performance Center, ils peuvent naviguer dans CA Performance Center, dans CA Network Flow Analysis et dans les sources de données enregistrées sans se connecter à nouveau.

Base d'informations de génération de rapports (RIB)

La *base d'informations de génération de rapports (RIB)* est un système de services Web et de fichiers XML que CA Infrastructure Management utilise pour décrire et fournir les données dans des vues et des tableaux de bord CA Performance Center. Ces données sont générées à partir de sources de données enregistrées dans l'instance CA Performance Center, comme CA Network Flow Analysis. La fonctionnalité de la base d'informations de génération de rapports fournit un environnement d'exploitation pour la génération de rapports tiers, fédérés et interproduit, et un service Web unique d'accès aux données avec des fonctionnalités semblables à SQL.

Console NFA

La *console NFA* est un composant dans un déploiement distribué de CA Network Flow Analysis qui fournit une interface utilisateur Web pour les rapports et les fonctions administratives. La console NFA crée des rapports à partir des données de présentation de l'entreprise, stockées localement, et à partir des données de résolution en 1 minute et 15 minutes récupérées d'autres composants.

Conversation

Une *conversation* est une session de trafic sous-réseau-à-sous-réseau ou utilisateur-à-utilisateur (hôte-à-hôte). La console NFA affiche les informations sur les conversations, afin de vous permettre de déterminer si une conversation cause par exemple une pointe de trafic sur une interface. Vous pouvez créer et exécuter des rapports pour identifier les principales conversations basées sur le volume.

Domaines IP

Les *domaines IP* sont des groupements logiques qui identifient des données collectées à partir d'unités et de réseaux divers. La surveillance par domaine signifie que les adresses IP avec des interfaces ou des applications associées qui appartiennent à différents réseaux de clients sont surveillées séparément. Lorsqu'ils sont combinés avec des autorisations appropriées, les domaines IP sont surveillés à partir d'une console unique, mais les opérateurs affichent seulement les données qui concernent les domaines qu'ils surveillent. Les administrateurs créent des domaines IP personnalisés dans la console CA Performance Center et affectent des Harvesters, des routeurs, des interfaces et des interfaces virtuelles personnalisées à des domaines IP dans la console NFA.

Données d'intervalle de 1 minute (haute résolution)

Les *données d'intervalle de 1 minute (haute résolution)* sont des informations détaillées collectées à partir de chaque Harvester et fournies à la console NFA pour leur affichage dans les vues et les rapports. Les données incluent les principaux protocoles pour chaque interface, le trafic pour les principaux hôtes et conversations, les principales conversations pour les principaux protocoles et les principaux protocoles, hôtes et conversations pour les principales valeurs de type de service. Les données d'intervalle de 1 minute sont stockées dans une base de données du serveur de Harvester, sous <chemin_installation_NFA>\Netflow\data\archive.

Droit du produit

Un *droit du produit* est un type d'autorisation associée à un compte d'utilisateur dans CA Performance Center. Les droits du produit permettent l'accès aux fonctionnalités de CA Performance Center, de CA Network Flow Analysis et de toutes les autres sources de données associées à l'instance CA Performance Center. Les administrateurs de CA Network Flow Analysis affectent des droits du produit à des comptes d'utilisateurs dans CA Performance Center.

DSA (appliance de stockage de données)

Un *DSA (appliance de stockage de données)* est un composant dans un déploiement d'architecture à trois niveaux de CA Network Flow Analysis. Chaque DSA de résolution en 15 minutes (historique) à partir de la console NFA et les stocke. Dans un déploiement d'architecture à deux niveaux, les données de résolution en 15 minutes sont traitées et stockées sur le Harvester.

Flux

Un *flux* est un ensemble de paquets IP qui traversent un point d'observation de réseau pendant une certaine période. Dans CA Network Flow Analysis 9.1.3, un flux peut être NetFlow v5, v7 ou v9 ; sFlow version 5 ; ou IPFIX, Jflow, cFlow ou le flux Huawei NetStream conforme aux normes pour NetFlow v5, v7 ou v9.

Groupe

Un *groupe* est une collection d'éléments gérés. Vous pouvez créer des groupes personnalisés dans CA Performance Center afin d'organiser logiquement les éléments gérés dans une arborescence, qui est ensuite propagée dans CA Network Flow Analysis. Les administrateurs globaux peuvent créer des groupes personnalisés d'éléments gérés, comme les applications, les serveurs, les réseaux, les routeurs et les interfaces, pour refléter le domaine de responsabilité de chaque utilisateur. Les administrateurs locaux de CA Network Flow Analysis et les opérateurs peuvent rechercher les éléments en fonction du groupe.

Groupes d'autorisations

Dans CA Performance Center, les *groupes d'autorisations* englobent la portée des éléments gérés que chaque utilisateur peut surveiller. Les administrateurs peuvent créer des groupes personnalisés d'éléments gérés, comme les applications, les serveurs, les réseaux, les routeurs et les interfaces, pour refléter le domaine de responsabilité de chaque utilisateur. Lorsqu'un administrateur de CA Network Flow Analysis affecte des groupes personnalisés à un compte d'utilisateur en tant qu'autorisations, les groupes personnalisés sont appelés groupes d'autorisation.

Harvester

Un *Harvester* est un composant dans un déploiement distribué de CA Network Flow Analysis qui collecte des flux bruts à partir des routeurs. Dans un déploiement d'architecture à deux niveaux, le Harvester traite et stocke les données de résolution en 1 minute et 15 minutes. Dans un déploiement d'architecture à trois niveaux, le Harvester traite et stocke les données de résolution en 1 minute. La console NFA récupère et traite les données de résolution en 15 minutes.

IIS

IIS est le serveur Web intégré à l'application Microsoft Windows Server. IIS consiste en plusieurs services, notamment Simple Mail Transfer Protocol (SMTP). Dans les versions d'IIS antérieures à 5.0, IIS est une abréviation d'Internet Information Server (serveur d'informations Internet). Dans la version 5.0 et les versions ultérieures, IIS est une abréviation d'Internet Information Services (services d'informations Internet).

Interface

Une *interface* est un point de connexion, comme un port série, un relais de trame, un port Fast Ethernet, un module de transfert asynchrone ou un circuit virtuel permanent. CA Network Flow Analysis génère des rapports sur les interfaces logiques activées sur un routeur pris en charge, pour lequel les flux sont activés. La console NFA affiche les interfaces surveillées dans votre environnement.

Interface utilisateur Web

L'interface utilisateur Web de CA Network Flow Analysis s'affiche comme la console NFA et permet à un opérateur d'accéder aux vues et aux rapports CA Network Flow Analysis à partir d'un navigateur Web. Les administrateurs de CA Network Flow Analysis utilisent cette interface pour effectuer certaines fonctions d'administration.

Interface virtuelle personnalisée

Une *interface virtuelle personnalisée* est une représentation abstraite d'une interface réseau, qui correspond à un ou plusieurs sous-réseaux d'interfaces physiques réelles. Les interfaces virtuelles personnalisées peuvent vous apporter une visibilité suffisante sur le trafic réseau pour un cloud porteur. Configurez des interfaces virtuelles personnalisées pour le trafic de centre de données transféré aux sous-réseaux à travers un cloud porteur MPLS lorsque le flux est activé sur les routeurs du centre de données.

Interruption

Une *interruption* est un message qui indique qu'un seuil a été atteint ou qu'une autre condition définie par l'utilisateur s'est produite. Un agent SNMP envoie des interruptions à la console NFA ou à un système de gestion de réseau. L'agent de l'outil de surveillance définit un nombre d'interruptions pour la gestion du système et des applications.

LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole logiciel permettant de localiser des organisations, des individus et d'autres ressources, telles que des fichiers et des périphériques dans un réseau. Le protocole LDAP est basé sur un modèle client/serveur. Le client LDAP établit une connexion de protocole TCP vers un serveur LDAP, puis envoie des demandes et reçoit des réponses via cette connexion.

Ligne de tendance

Une *ligne de tendance* est une projection des performances à venir d'un élément en fonction des performances passées. CA Network Flow Analysis crée la ligne de tendance comme la meilleure ligne droite reliant les points de données de la période de référence.

Mappage d'applications

Le *mappage d'applications* est une technique basée sur des règles pour regrouper le trafic d'une application afin de faciliter la génération de rapports sur celle-ci. Les règles de mappage d'applications sont définies selon des facteurs qui peuvent inclure l'origine du trafic (hôte, sous-réseau et masque, et/ou port), le type de service et le protocole.

NetFlow

NetFlow est une transaction entre deux hôtes, qui utilise une paire unique de numéros de port et d'adresses IP et inclut certaines informations de trafic réseau. Vous pouvez configurer un routeur Cisco pour exporter des informations de flux en envoyant des paquets UDP qui contiennent des statistiques de flux à un ou plusieurs collecteurs, comme les composants de collectes. CA Network Flow Analysis prend en charge les versions 5, 7 et 9 de NetFlow, et la version 5 de sFlow. CA Network Flow Analysis prend également en charge les flux IPFIX, Jflow, cFlow et Huawei NetStream s'ils sont conformes aux normes de NetFlow 5, 7 ou 9.

Pare-feu

Un serveur de *pare-feu* est une passerelle entre un réseau local et un grand réseau non sécurisé, comme Internet. Un serveur de pare-feu exécute généralement un package logiciel qui inspecte les paquets entrants et sortants et décide de les laisser passer ou pas.

Période de génération de rapports

Une *période de génération de rapports* représente la période spécifiée par l'utilisateur à inclure dans un rapport CA Network Flow Analysis. Les options temporelles varient en fonction du type de rapport et peuvent être des heures, des jours, des semaines ou des mois.

Places réservées

Les *places réservées* sont une technique basée sur des règles permettant de garantir que les rapports incluent le trafic approprié, même si le volume ou le taux de trafic est faible. Les règles créent des places réservées dans des rapports pour les données qui correspondent aux ports et aux protocoles cibles.

Profils SNMP

Les *profils SNMP* sont des définitions qui contiennent les informations nécessaires pour activer des requêtes sécurisées de MIB d'unité à l'aide de SNMP. Chaque connexion à une unité est effectuée à l'aide d'un des profils SNMP stockés dans CA Performance Center. Les administrateurs de CA Network Flow Analysis peuvent créer des profils SNMP dans CA Performance Center le cas échéant.

Rapport

Un *rapport* est un affichage de données collectées, que vous affichez dans la console NFA à partir des pages Présentation d'entreprise, Interfaces, Génération de rapports personnalisés, Examen des flux et Analyse. Vous pouvez imprimer ou enregistrer les rapports au format PDF. Vous pouvez également exporter les rapports dans des fichiers CSV. Un administrateur peut configurer l'envoi par courriel de certains rapports à des intervalles planifiés.

Rapport d'analyse en profondeur

Un *rapport d'analyse en profondeur* dans une page Interfaces est une vue des données détaillées d'une interface. Pour afficher un rapport d'analyse en profondeur d'une interface, sélectionnez Interfaces dans le menu de la console NFA, puis cliquez sur un lien d'interface. Vous pouvez également afficher ce type de rapport en cliquant sur un lien d'interface dans un tableau de bord CA Performance Center ou dans d'autres types de vues CA Network Flow Analysis.

Référence

Une *référence* est l'enregistrement d'un comportement typique, calculé à partir des comportements précédents. Les références vous aident à comparer les modifications dans le temps et à prévoir les données ou les performances futures. La comparaison des valeurs actuelles aux projections de la référence permet de déterminer si les valeurs actuelles sont habituelles. La référence dans un graphique de tendance est calculée à l'aide des données des six semaines précédant la plage de dates sélectionnée, à l'exception des points de données déjà inclus dans le graphique.

Rôle

Un *rôle* est un paramètre qu'un administrateur de CA Network Flow Analysis affecte à un compte d'utilisateur, qui contrôle l'accès utilisateur aux fonctionnalités de produit CA Network Flow Analysis et aux pages de tableau de bord de CA Performance Center. Un rôle peut également accorder un accès administratif à la configuration du produit. Dans un déploiement bien planifié, les rôles permettent aux utilisateurs d'accéder aux fonctionnalités dont ils ont besoin pour effectuer leurs tâches et limitent leur accès aux fonctionnalités dont ils n'ont pas besoin.

SMTP

Le *protocole Simple Mail Transfer Protocol (SMTP)* est le protocole TCP/IP (Transfer Control Protocol/Internet Protocol) utilisé pour l'envoi et la réception de courriels sur les réseaux de données.

SNMP

Le *Simple Network Management Protocol (SNMP)* est le protocole de gestion de réseaux utilisé presque exclusivement sur les réseaux de données. Il s'agit d'une méthode de surveillance et de contrôle des périphériques réseau, mais également de gestion des configurations, de la collecte des statistiques, des performances et de la sécurité.

Sources de données

Les sources de données sont les produits pris en charge, comme CA Network Flow Analysis, qui fournissent les données de performances pour affichage dans CA Performance Center. Les sources de données fournissent également certaines données de configuration qui sont stockées dans CA Performance Center. CA Network Flow Analysis effectue la surveillance, la collecte des données, le cumul des données et d'autres tâches. Certaines de ces tâches sont effectuées indépendamment, mais une fois qu'une instance de CA Network Flow Analysis est enregistrée dans une instance CA Performance Center, l'instance CA Network Flow Analysis est référencée comme source de données.

Synchronisation

La *synchronisation*, ou la synchronisation globale, est un processus automatique dans CA Performance Center, au cours duquel des informations provenant de CA Network Flow Analysis et d'autres sources de données sont reçues et traitées. La synchronisation se produit toutes les 5 minutes et inclut les données de configuration et de performances provenant de toutes les sources de données enregistrées.

Index

1

- 15 minutes, données d'historique
 - 15 minutes, données d'historique (administrateur)
 - base de données - 150
 - perte lors de la suppression d'un routeur - 71
 - restauration - 157
 - sauvegarde - 155
 - types de données collectées - 145
- activation (administrateur)
 - interfaces (interfaces actives) - 34
 - NetFlow sur des routeurs - 29
- actualisation
 - noms de DNS (administrateur) - 114
- Administration (administrateur)
 - Configuration de l'adresse ou du nom d'hôte, page - 114
 - Configuration des interruptions, page - 107
 - Configuration des périodes de génération de rapports, page - 101
 - Configuration du filtre de temps, page - 99
 - Configuration du groupe de protocoles, page - 86
 - Configuration du groupe de types de service, page - 91
 - Configuration du type de service, page - 90
 - Définitions d'application, mappage d'applications - 128
 - Définitions d'application, places réservées - 129, 130
 - Interfaces actives, page - 98, 131, 132
 - Interfaces de cumul, page - 79
 - Interfaces disponibles, page - 135
 - Modèles d'interface, page - 82
 - page DSA (à 3 niveaux) - 136
 - Paramètres de l'outil de surveillance, page - 104
 - Statut du système/page d'accueil par défaut - 61, 106
- Administration, options du menu (administrateur)
 - Activer les interfaces (système) - 133
 - Adresses (génération de rapports) - 114
 - Alertes - 107
 - aperçu - 61
 - Composant de collecte (système) - 26
 - Cumuls (interfaces) - 79
 - Définitions d'application - 122, 124, 125, 126, 128
 - Filtres de temps (génération de rapports) - 99
 - Groupe de protocoles (groupes) - 86
 - Groupe de types de service (Groupes) - 91
 - Modèles (système) - 82
 - Noms de type de service (définir une application) - 90
 - Paramètres de l'outil de surveillance (intégrité) - 104
 - périodes de génération de rapports (génération de rapports) - 101
 - Physique et virtuelle (interfaces) - 66, 98, 132
 - Statut du système (intégrité) - 106
- adresses
 - adresses électroniques de l'outil de surveillance (administrateur) - 104
 - Configuration de l'adresse ou du nom d'hôte (administrateur) - 114
 - expiration, motif (administrateur) - 114
 - modification de l'adresse IP du composant de collecte (administrateur) - 75
 - modification pour le DSA actuel (administrateur) - 137
 - modification pour le nouveau DSA (administrateur) - 138
- affichage
 - statut de composant (administrateur) - 61
- affichage (administrateur)
 - noms d'interface (afficher le nom de l'unité) - 85
- Afficher le nom de l'unité, option (administrateur)
 - résultats de la définition - 85
- ajout
 - Ajouter des places réservées, boîte de dialogue (administrateur) - 129
 - Ajouter un composant de collecte, boîte de dialogue (administrateur) - 26
 - Ajouter un DSA, boîte de dialogue (administrateur) - 30

Ajouter un mappage d'applications, boîte de dialogue (administrateur) - 122, 124, 125, 126

Ajouter une définition d'interruption, page (administrateur) - 107

Ajouter une interface virtuelle personnalisée, boîte de dialogue (administrateur) - 54

Chaîne de communauté (administrateur) - 104

Chaîne de communauté d'interruptions (administrateur) - 104

Composants de collecte (administrateur) - 26

comptes d'utilisateurs (administrateur) - 39

domaines personnalisés (administrateur) - 24

groupes personnalisés (CA PC) (administrateur) - 49

interfaces à des cumuls (administrateur) - 79

profils SNMP (administrateur) - 19

rôles pour les utilisateurs (administrateur) - 43

valeurs de type de service aux groupes (administrateur) - 92

annulation de l'enregistrement (administration) résultats - 51

appliance de stockage des données (DSA) [à 3 niveaux] (administrateur)

ajout - 30

ajout de corrections - 32

chaîne de communauté pour l'outil de surveillance - 104

modification de l'adresse pour le DSA actuel - 137

modification de l'adresse pour le nouveau DSA - 138

révision du statut - 106

architecture à trois niveaux (administrateur)

modification de l'adresse pour le DSA actuel - 137

modification de l'adresse pour le nouveau DSA - 138

autorisations (administrateur)

affectation d'autorisations aux utilisateurs - 46

avertissements (administrateur)

Icône d'avertissement (page Statut du système) - 106

plus de détails - 106

pour les composants - 106

base de données - 150

base de données de composant de collecte (administrateur)

emplacement - 150

port correspondant au port d'écoute de flux - 29

restauration - 157

sauvegarde - 155

base de données de l'interrogateur (administrateur)

emplacement - 150

restauration - 157

sauvegarde - 155

base de données du générateur de rapports (administrateur)

emplacement - 150

bases de données (administrateur)

emplacements - 150

sauvegarde des composants de bases de données - 148

boîtes de dialogue

Ajouter des places réservées (administrateur) - 129

Ajouter un composant de collecte (administrateur) - 26

Ajouter un DSA, boîte de dialogue (administrateur) - 30

Ajouter un mappage d'applications (administrateur) - 122, 124, 125, 126

Ajouter une interface virtuelle personnalisée (administrateur) - 54

Confirmation de la fusion des interfaces (administrateur) - 132

Index de groupe de types de service (administrateur) - 90

Index des types de service (administrateur) - 92

Modifier le routeur (administrateur) - 98

Modifier les interfaces (administrateur) - 81

Modifier les places réservées (administrateur) - 130

Modifier l'interface/le routeur (administrateur) - 70

Modifier une interface virtuelle personnalisée (administrateur) - 70

CA Performance Center (administrateur)

affectation d'autorisations aux utilisateurs - 46

affichage de la liste des comptes d'utilisateurs - 38

-
- affichage de profils SNMP - 17
 - ajout de comptes d'utilisateurs - 39
 - ajout de domaines personnalisés - 24
 - ajout de groupes personnalisés - 49
 - ajout de profils SNMP - 19
 - ajout de rôles pour les utilisateurs - 43
 - effet de l'affectation d'un client hébergé - 24
 - enregistrement de NFA - 15
 - test des connexions à la source de données - 17
 - cFlow
 - prise en charge - 29
 - Chaîne de communauté, paramètre (administrateur)
 - définition pour l'outil de surveillance - 104
 - chaînes SNMP (administrateur)
 - Chaîne de communauté pour l'outil de surveillance - 104
 - changement de nom routeurs - 98
 - chemins d'accès (administrateur)
 - journaux, chemin de configuration des journaux/services - 118
 - clients hébergés
 - effet de l'affectation - 24
 - vérification du client hébergé du Harvester - 28
 - commandes (administrateur)
 - configuration de NetFlow - 29
 - configuration de persistance d'index - 29
 - enregistrement de la configuration dans la mémoire statique - 29
 - composants de CA Network Flow Analysis surveillance (administrateur) - 103
 - Composants de collecte (administrateur)
 - ajout d'un composant de collecte - 26
 - chaîne de communauté pour l'outil de surveillance - 104
 - modification de domaines, d'adresses, de descriptions - 75
 - présentation du rôle de collecte de données - 141
 - révision du statut de Harvester - 106
 - services/journaux installés sur les serveurs - 118
 - suppression d'un composant de collecte - 74
 - vérification du domaine/client hébergé - 28
 - configuration (administrateur)
 - exportation des données de systèmes autonomes vers NetFlow - 95
 - Instructions relatives à l'outil de clonage de paquets de flux - 58
 - interruptions pour les outils externes - 113
 - NetFlow, commandes - 29
 - présentation de configuration d'interruptions - 37
 - configuration matérielle requise (administrateur)
 - moteur pour les commutateurs Catalyst - 29
 - connexion (administrateur)
 - nom d'utilisateur/mot de passe par défaut - 26
 - Conserver le protocole de mappage ToS, option (administrateur)
 - effets sur le mappage d'applications - 122
 - Console NFA
 - avertissements (administrateur) - 106
 - base de données de configuration (administrateur) - 150
 - présentation du rôle de traitement de données - 141
 - restauration des données de configuration (administrateur) - 157
 - révision du statut de console - 106
 - rôle de traitement de données - 141
 - sauvegarde de la configuration (administrateur) - 155
 - services/journaux installés (administrateur) - 118
 - courriel
 - adresse pour l'outil de surveillance (administrateur) - 104
 - création
 - cumuls d'interface (administrateur) - 79
 - étiquettes de type de service (administrateur) - 90
 - filtres de temps (administrateur) - 99
 - groupes de protocoles (administrateur) - 86
 - groupes de types de service (administrateur) - 91
 - interfaces virtuelles personnalisées (administrateur) - 54
 - interruptions (administrateur) H - 107
 - modèles d'interface (administrateur) - 82
 - périodes de génération de rapports (administrateur) - 101
 - Règles de places réservées (administrateur) - 129
-

- cumuls d'interface (administrateur)
 - création - 79
 - effets de la suppression de routeurs - 71
 - modification - 80
 - modification de plusieurs cumuls - 81
 - suppression - 82
 - utilisations - 78
- Définitions d'application, page (administrateur)
 - Mappage d'applications - 127, 128
 - Places réservées - 129, 130
- défragmentation (administrateur)
 - avertissement sur la défragmentation - 158
- démarrage
 - services, ordre (administrateur) - 155
- dépannage
 - ajout de DSA (administrateur) - 32
 - interruptions intégrées (administrateur) - 114
 - protection de l'intégrité des données (administrateur) - 158
- désactivation (administrateur)
 - affichage des interfaces dans les rapports - 135
 - interfaces (page Interfaces actives) - 34, 133
 - rapports, par la suppression de routeurs - 71
 - surveillance générée par un routeur - 52
- développement (administrateur)
 - détails de routeur - 72
 - Interfaces actives, affichage de la page - 132
- documentation
 - adresse pour les commentaires - 5
 - emplacement/liste - 4
 - Manuel de l'authentification unique - 13
- domaines (administrateur)
 - affichage de la liste - 23
 - ajout de domaines personnalisés - 24
 - Configuration de l'adresse ou du nom d'hôte, page - 114
 - définition du domaine de l'interface/de l'interface virtuelle personnalisée - 70
 - effets sur les valeurs de type de service - 90
 - exclusion des routeurs de l'affichage - 52
 - modification du domaine de l'interface/de l'interface virtuelle personnalisée - 70
 - modification du domaine du composant de collecte (administrateur) - 26
 - vérification du domaine du composant de collecte - 28
- données
 - architecture de collecte de données - 141

- configuration de la collecte de flux (présentation) (administrateur) - 25
- garantie de l'intégrité (administrateur) - 158
- types de données collectés d'intervalle de 1 minute - 147
- types de données collectés d'intervalle de 15 minutes - 145
- données de configuration (administrateur)
 - base de données de configuration de console NFA - 150
 - conventions de fichier FlowCloneDef.ini - 60
 - emplacements de fichiers de configuration de Harvester - 150
 - enregistrement dans la mémoire statique - 29
 - exemple de fichier FlowCloneDef.ini - 59
 - fichiers de configuration pour les journaux/services - 118
 - restauration des données de configuration de console - 157
 - sauvegarde automatique - 155
 - sauvegarde manuelle des données de console - 155
- données de présentation d'entreprise (administrateur)
 - base de données - 150
 - types de données/durée de stockage - 144
- données de système autonome
 - modification de noms de systèmes autonomes (administrateur) - 97
 - personnalisation des noms de système autonomes (administrateur) - 95
 - révision des noms de systèmes autonomes (administrateur) - 96
- données d'historique, 15 minutes (administrateur)
 - emplacement de base de données - 150
 - restauration - 157
 - sauvegarde - 155
 - types de données collectées - 145
- données d'intervalle de 1 minute (administrateur)
 - base de données - 150
 - restauration - 157
 - sauvegarde - 155
 - types de données collectées - 147
- données IPFIX (administrateur)
 - prise en charge - 29
- droits

- affectation de droits de produit à des utilisateurs - 48
- enregistrement (administrateur)
 - source de données - 15
 - test des connexions à la source de données - 17
- étiquetage (administrateur)
 - valeurs de type de service - 90
- Examen des flux, page
 - définition d'emplacement/de niveau du journal (administrateur) - 118
 - données à partir de l'activation des interfaces (administrateur) - 133
- expiration (administrateur)
 - adresses IP expirées, motif - 114
- exportation (administrateur)
 - rapports sous forme de fichiers CSV, activation - 52
- fichier MIB (administrateur)
 - accès/valeurs contenues - 113
- fichiers CSV (valeurs séparées par des virgules)
 - ajout de la console aux sites de confiance (administrateur) - 52
- filtres de temps
 - création (administrateur) - 99
 - utilisation dans les interruptions (administrateur) - 107
- flux
 - types pris en charge - 29
- fusion (administrateur)
 - Confirmation de la fusion des interfaces, boîte de dialogue - 132
 - interfaces - 132
 - interfaces, motifs/résultats - 132
- groupes
 - ajout de groupes personnalisés (CA PC) - 49
 - création de groupes de protocoles (administrateur) - 86
 - suppression/modification par annulation d'enregistrement (administrateur) - 51
- groupes de protocoles
 - création (administrateur) - 86
- Groupes de types de service
 - Configuration du groupe de types de service, page (administrateur) - 91
 - création (administrateur) - 91
 - modification du contenu (administrateur) - 93
 - suppression (administrateur) - 94
- groupes d'interfaces

- effets de l'annulation d'enregistrement dans CAPC (administrateur) - 51
- Harvesters
 - brève description - 141
- hôtes
 - Règle de mappage d'applications d'hôte (administrateur) - 125
- installation (administrateur)
 - fonctionnalité de l'outil de clonage de flux - 58
 - tâches de post-installation - 52
- interfaces
 - activation, motifs (administrateur) - 133
 - activation/désactivation (interfaces actives) (administrateur) - 133
 - Confirmation de la fusion des interfaces (administrateur) - 132
 - définition du format de nom (administrateur) - 85
 - désactivation pour les rapports (administrateur) - 135
 - fusion (administrateur) - 132
 - fusion, motifs (administrateur) - 132
 - Interfaces actives, tâches de la page (administrateur) - 131
 - modification dans la page Interfaces actives (administrateur) - 70
 - perte lors de la suppression d'un routeur (administrateur) - 71
 - présentation des interfaces virtuelles personnalisées (administrateur) - 54
 - recherche dans la page Interfaces actives (administrateur) - 69
 - standardisation des noms à l'aide de modèles (administrateur) - 82
 - suppression (administrateur) - 135
 - vérification de la visibilité (console NFA) - 35
 - vérification de l'activation (administrateur) - 34
 - vérification des vitesses, but (administrateur) - 52
- Interfaces actives, page (administrateur)
 - affichage des interfaces physiques et virtuelles - 66
 - création/configuration des interfaces virtuelles personnalisées - 54
 - fusion d'interfaces - 132
 - modification des détails - 70
 - personnalisation de l'apparence - 72

-
- présentation des tâches - 131
 - recherche de
 - routeurs/d'interfaces/d'interfaces virtuelles personnalisées - 69
 - suppression de routeurs - 71
 - suppression d'interfaces - 135
 - interfaces de bouclage (administrateur)
 - configuration pour l'exportation NetFlow - 29
 - Interfaces de cumul, page (administrateur)
 - création de cumuls - 79
 - modification des cumuls - 80, 81
 - suppression de cumuls - 82
 - Interfaces disponibles, page (administrateur)
 - activation/désactivation des interfaces - 133
 - persistance des routeurs supprimés - 71
 - suppression d'interfaces des rapports - 135
 - interfaces virtuelles (administrateur)
 - voir interfaces virtuelles personnalisées - 54
 - interfaces virtuelles personnalisées (administrateur)
 - aperçu - 54
 - création - 54
 - exemple - 56
 - Interfaces actives, tâches de la page - 131
 - modification dans la page Interfaces actives - 70
 - perte lors de la suppression d'un routeur - 71
 - priorités - 56
 - recherche dans la page Interfaces actives - 69
 - résultats de la suppression - 54
 - interrogation (administrateur)
 - délai d'expiration pour l'unité SNMP (outil de surveillance) - 104
 - nouvelles tentatives pour l'unité SNMP (outil de surveillance) - 104
 - paramètres du port d'écoute de Harvester/d'écouteur de flux correspondant - 29
 - interruptions (administrateur)
 - configuration pour les outils externes - 113
 - création - 107
 - définition de la destination (outil de surveillance) - 104
 - dépannage d'interruption intégrée - 114
 - Destination d'interruption, paramètre (outil de surveillance) - 104
 - emplacement du fichier MIB - 113
 - informations sur les interruptions, présentation - 112
 - perte lors de la suppression d'un routeur - 71
 - présentation de la configuration - 37
 - Intervalle de contrôle du système (administrateur)
 - définition pour l'outil de surveillance - 104
 - J-Flow
 - prise en charge - 29
 - journaux (administrateur)
 - noms/emplacements/fichiers de configuration des journaux - 118
 - Journaux de composant de collecte (administrateur)
 - définition d'emplacement/de niveau - 118
 - LDAP (administrateur)
 - pris en charge par l'outil d'authentification unique - 13
 - logiciels tiers
 - droits/contrats de licence - 11
 - maintenance (administrateur)
 - CA Network Flow Analysis - 103
 - données collectées - 141
 - Mappage d'applications (administrateur)
 - aperçu - 121
 - modification de règles - 127
 - paramètres globaux - 122
 - priorité des règles - 122
 - Règle de sous-réseau - 122, 124
 - Règle d'hôte - 125
 - règle Tout (type de service) - 126
 - suppression de règles - 128
 - modèles (administrateur)
 - modification du modèle de routeur - 70
 - modification
 - adresse pour le DSA actuel (administrateur) - 137
 - adresse pour le nouveau DSA (administrateur) - 138
 - contenu du groupe de types de service (administrateur) - 93
 - cumul d'interfaces (administrateur) - 80
 - cumuls de plusieurs interfaces (administrateur) - 81
 - détails du composant de collecte (administrateur) - 75
 - Modifier le routeur, boîte de dialogue (administrateur) - 70, 98
 - Modifier les interfaces, boîte de dialogue (administrateur) - 81

-
- Modifier les places réservées, boîte de dialogue (administrateur) - 130
 - Modifier l'interface, boîte de dialogue (administrateur) - 70
 - Modifier une interface virtuelle personnalisée, boîte de dialogue (administrateur) - 70
 - nombre de détails affichés (administrateur) - 73
 - noms de routeur (administrateur) - 98
 - Paramètres de l'outil de surveillance (administrateur) - 104
 - paramètres de rapport, but (administrateur) - 52
 - Règles de mappage d'applications (administrateur) - 127
 - Règles de places réservées (administrateur) - 130
 - routeurs/interfaces (administrateur) - 70
 - MySQL (administrateur)
 - emplacement du service MySql51 - 118
 - journal de NQMySql51 (oursql_5.1_error.log) - 118
 - N principaux groupes (administrateur)
 - génération de rapports sur les protocoles non N principaux - 128
 - NetFlow (administrateur)
 - activation de l'exportation des données de systèmes autonomes - 95
 - configuration, versions prises en charge - 29
 - Nfharvestererrors.log (administrateur)
 - définition d'emplacement/de niveau - 118
 - nommage/renommage
 - routeurs (administrateur) - 98
 - valeurs de type de service (administrateur) - 90
 - noms de DNS (administrateur)
 - actualisation des adresses expirées - 114
 - notifications (administrateur)
 - des interruptions (outil de surveillance) - 104
 - des violations de seuil (outil de surveillance) - 104
 - NQMgmtSrvErrors.log (administrateur)
 - définition d'emplacement/de niveau - 118
 - nqservErrors.log (administrateur)
 - définition d'emplacement/de niveau - 118
 - Outil d'authentification unique (administrateur)
 - brève description - 13
 - informations pour l'enregistrement dans CA PC - 15
 - Outil de clonage de flux
 - conventions de fichier de configuration - 60
 - exemple de configuration - 59
 - installation - 58
 - instructions relatives à la configuration - 58
 - paquets NetFlow - 57
 - restrictions relatives aux paquets IP clonés - 60
 - Outil de surveillance (administrateur)
 - description de services - 116
 - journal - 118
 - Paramètres de l'outil de surveillance, page - 104
 - Paramètres de l'application, page (administrateur)
 - Afficher le nom de l'unité, option - 85
 - performances (administrateur)
 - ajustement des paramètres de rapport - 52
 - périodes de génération de rapports
 - création (administrateur) - 101
 - motifs de la création (administrateur) - 101
 - persistance d'index (administrateur)
 - configuration des routeurs - 29
 - personnalisation (administrateur)
 - apparence de la page Interfaces actives - 72
 - CA Network Flow Analysis - 77
 - perte lors de la suppression d'un routeur - 71
 - Places réservées (administrateur)
 - création de règles - 129
 - modification de règles - 130
 - suppression de règles - 130
 - utilisation - 128
 - Pompage de l'émission ou de la multidiffusion (administrateur)
 - désactivation de la surveillance de routeur - 52
 - Port de redirection TCP (administrateur)
 - effets sur le mappage d'applications - 122
 - Port de redirection UDP (administrateur)
 - effets sur le mappage d'applications - 122
 - ports (administrateur)
 - génération de rapports avec places réservées - 129
 - modification pour des routeurs - 70
 - priorités (administrateur)
 - noms d'unité/d'interface - 82
-

Priorités de l'interface virtuelle personnalisée - 56	désactivation de routeurs (administrateur) - 71
règle de mappage d'applications, priorités - 122	Groupes de types de services, boîte de dialogue (administrateur) - 91
profils SNMP (administrateur)	RealtimeReaperErrors.log (administrateur)
affichage de liste dans CA PC - 17	définition d'emplacement/de niveau - 118
modification du profil/de la version pour un routeur - 70	recherche
protocoles (administrateur)	routeurs/interfaces (administrateur) - 69
création d'interruptions - 107	redémarrage (administrateur)
génération de rapports avec places réservées - 129	services, ordre de redémarrage - 155
rapports	règles (administrateur)
activation de l'exportation au format CSV (administrateur) - 52	Places réservées, création - 129
création de filtres de temps (administrateur) - 99	Places réservées, présentation - 128
création de groupes de protocoles (administrateur) - 86	Règle de mappage d'applications de sous-réseau - 122, 124
création de groupes de types de service (administrateur) - 91	Règle de mappage d'applications d'hôte - 125
création de périodes de génération de rapports (administrateur) - 101	règle de mappage d'applications Tout (type de service) - 126
création d'étiquettes de types de service (administrateur) - 90	règle de mappage d'applications, priorités - 122
désactivation d'interfaces (administrateur) - 135	restauration - 157
protocoles/ports (administrateur) - 128	restauration (administrateur)
Rapports d'analyse	bases de données - 157
boîte de dialogue affichant les groupes de types de service (administrateur) - 91	rôles (administrateur)
création de filtres de temps (administrateur) - 99	ajout pour les utilisateurs - 43
création de groupes de types de service (administrateur) - 91	routeurs
rapports de la page Interface	activation de NetFlow (administrateur) - 29
création de filtres de temps - 99	configuration (administrateur) - 29
création de périodes de génération de rapports (administrateur) - 101	configuration de la persistance d'index (administrateur) - 29
types de rapport avec des périodes de génération de rapports (administrateur) - 101	désactivation de la surveillance (administrateur) - 52
Rapports personnalisés	développement des détails (administrateur) - 72
création de filtres de temps (administrateur) - 99	Interfaces actives, tâches de la page (administrateur) - 131
création de groupes de protocoles (administrateur) - 86	modification dans la page Interfaces actives (administrateur) - 70
création de groupes de types de service (administrateur) - 91	nombre de/détails affichés (administrateur) - 73
	recherche dans la page Interfaces actives (administrateur) - 69
	renommage (administrateur) - 98
	suppression, des interfaces actives (administrateur) - 71
	sauvegarde - 155
	sauvegarde (administrateur)
	bases de données - 155
	Serveur de gestion (administrateur)

journal (NQMgmtSrvErrors) - 118
service de base d'informations de génération de rapports (administrateur)
 emplacement du journal de service de base d'informations de génération de rapports de CA NFA - 118
Service de génération de rapports (administrateur)
 description - 116
 noms/emplacements des journaux - 118
Service de gestionnaire (administrateur)
 description - 116
 journal - 118
Service de pompage (administrateur)
 description - 116
 journal (PumpLog.log) - 118
Service de rapport (administrateur)
 journal (FlowForensicsLog.log) - 118
services (administrateur)
 brève description - 116
 emplacements/journaux/fichiers de configuration - 118
Services de requête (administrateur)
 définition d'emplacement/de niveau du journal - 118
Services généraux (administrateur)
 description - 116
 journal (nqservErrors) - 118
Seuil de disque, paramètre (administrateur)
 définition pour l'outil de surveillance - 104
Seuil de la mémoire, paramètre (administrateur)
 définition pour l'outil de surveillance - 104
Seuil d'UC, paramètre (administrateur)
 définition pour l'outil de surveillance - 104
seuils
 création d'interruptions (administrateur) - 107
 disque - outil de surveillance (administrateur) - 104
 interruptions/alertes NFA (administrateur) - 107
 notifications (outil de surveillance) (administrateur) - 104
 UC - outil de surveillance (administrateur) - 104
 utilisation de la mémoire (outil de surveillance) (administrateur) - 104
sFlow
 version prise en charge - 29

sous-réseaux (administrateur)
 modification de la description de l'interface virtuelle personnalisée - 70
 Règle de mappage d'applications de sous-réseau - 122, 124
status
 vérification pour les composants (administrateur) - 61, 106
Statut du système, page (administrateur)
 ouverture/utilisation - 61
support technique
 Portail de self-service de CA - 5
suppression
 Composants de collecte (administrateur) - 74
 cumuls d'interface (administrateur) - 82
 groupes de protocoles (administrateur) - 86
 groupes de types de service (administrateur) - 94
 groupes/utilisateurs par annulation d'enregistrement (administrateur) - 51
 interfaces (administrateur) - 135
 protocoles d'un groupe (administrateur) - 86
 Règles de mappage d'applications (administrateur) - 128
 Règles de places réservées (administrateur) - 130
 résultats pour les interfaces virtuelles personnalisées (administrateur) - 54
 routeurs, des interfaces actives (administrateur) - 71
surveillance (administrateur)
 composants - 103
test
 connexion à la source de données - 17
Type de service
 Configuration du groupe de types de service, page (administrateur) - 91
 création d'interruptions (administrateur) - 107
 effets du masque de type de service sur le mappage d'applications (administrateur) - 122
 étiquettes de type de service, création (administrateur) - 90
 Index des types de service, boîte de dialogue (administrateur) - 92
 Règle de mappage d'applications (administrateur) - 126
types de données collectées - 145

- unités SNMP (administrateur)
 - Délai d'expiration SNMP, paramètre (outil de surveillance) - 104
 - Nouvelles tentatives SNMP, paramètre (outil de surveillance) - 104
- utilisateurs (administrateur)
 - affectation d'autorisations - 46
 - affectation de droits de produit - 48
 - affichage de la liste des comptes d'utilisateurs - 38
 - ajout de comptes d'utilisateurs - 39
 - ajout de rôles - 43
 - création de comptes d'utilisateurs, but - 52
 - suppression par annulation d'enregistrement - 51
- utilisation de la mémoire (administrateur)
 - modification du seuil de l'outil de surveillance - 104
- vérification (administrateur)
 - domaine du composant de collecte - 28
 - interfaces activées - 34
 - statut de composant - 106
 - visibilité d'interface (console NFA) - 35
 - vitesse des interfaces, but - 52
- vitesse en entrée/en sortie (administrateur)
 - modification d'interfaces/d'interfaces virtuelles personnalisées - 70
- vitesse en sortie/en entrée (administrateur)
 - modification d'interfaces/d'interfaces virtuelles personnalisées - 70
- volume
 - générations de rapports sur les protocoles à faible volume (administrateur) - 129

A

- activation
 - interfaces (interfaces actives) - 34
 - NetFlow sur des routeurs - 29
- actualisation
 - noms de DNS pour les adresses expirées - 114
- Administration
 - Configuration de l'adresse ou du nom d'hôte, page - 114
 - Configuration des interruptions, page - 107
 - Configuration des périodes de génération de rapports, page - 101
 - Configuration du filtre de temps, page - 99
 - Configuration du groupe de protocoles, page - 86

- Configuration du groupe de types de service, page - 91
- Configuration du type de service, page - 90
- Définitions d'application, mappage d'applications - 128
- Définitions d'application, places réservées - 129, 130
- Interfaces actives, page - 98, 131, 132
- Interfaces de cumul, page - 79
- Interfaces disponibles, page - 135
- Modèles d'interface, page - 82
- page DSA (à 3 niveaux) - 136
- Paramètres de l'outil de surveillance, page - 104
- Statut du système/page d'accueil par défaut - 61, 106
- Administration, options du menu
 - Activer les interfaces (système) - 133
 - Adresses (génération de rapports) - 114
 - Alertes - 107
 - aperçu - 61
 - Composant de collecte (système) - 26
 - Cumuls (interfaces) - 79
 - Définitions d'application - 122, 124, 125, 126, 128
 - Filtres de temps (génération de rapports) - 99
 - Groupes de protocoles (groupes) - 86
 - Groupes de types de service (Groupes) - 91
 - Modèles (système) - 82
 - Noms de type de service (définir une application) - 90
 - Paramètres de l'outil de surveillance (intégrité) - 104
 - périodes de génération de rapports (génération de rapports) - 101
 - Physique et virtuelle (interfaces) - 66, 98, 132
 - Statut du système (intégrité) - 106
- adresses
 - adresses électroniques (outil de surveillance) - 104
 - Configuration de l'adresse ou du nom d'hôte, page - 114
 - expiration, motif - 114
 - modification du nouveau DSA - 138
 - modification pour le DSA actuel - 137
- affichage
 - noms d'interface (afficher le nom de l'unité) - 85
- Afficher le nom de l'unité, option
 - résultats de la définition - 85
- ajout

- Ajouter des places réservées, boîte de dialogue - 129
- Ajouter un composant de collecte, boîte de dialogue - 26
- Ajouter un DSA, boîte de dialogue - 30
- Ajouter un mappage d'applications, boîte de dialogue - 124, 125, 126
- Ajouter une définition d'interruption, page - 107
- Ajouter une interface virtuelle personnalisée, boîte de dialogue - 54
- Chaîne de communauté (outil de surveillance) - 104
- Chaîne de communauté d'interruption (outil de surveillance) - 104
- comptes d'utilisateurs - 39
- domaines personnalisés - 24
- groupes personnalisés (CA PC) - 49
- interfaces à des cumuls - 79
- Profils SNMP - 19
- rôles pour les utilisateurs - 43
- valeurs de type de service aux groupes - 92
- annulation de l'enregistrement résultats - 51
- appliance de stockage des données (DSA) [à 3 niveaux]
 - ajout - 30
 - ajout de corrections - 32
 - chaîne de communauté pour l'outil de surveillance - 104
 - modification de l'adresse pour le DSA actuel - 137
 - modification de l'adresse pour le nouveau DSA - 138
 - révision du statut - 106
- architecture à trois niveaux
 - modification de l'adresse pour le DSA actuel - 137
 - modification de l'adresse pour le nouveau DSA - 138
- autorisations
 - affectation d'autorisations aux utilisateurs - 46
- avertissements
 - Icône d'avertissement (page Statut du système) - 106
 - plus de détails - 106
 - pour les composants - 106

B

- base de données de composant de collecte
 - emplacement - 150

- port correspondant au port d'écoute de flux - 29
 - restauration - 157
 - sauvegarde - 155
- base de données de générateur de rapports
 - emplacement - 150
- base de données de l'interrogateur
 - emplacement - 150
 - restauration - 157
 - sauvegarde - 155
- bases de données
 - emplacements - 150
 - sauvegarde des composants de bases de données - 148
- boîtes de dialogue
 - Ajouter des places réservées - 129
 - Ajouter un composant de collecte - 26
 - Ajouter un DSA, boîte de dialogue - 30
 - Ajouter un mappage d'applications - 122, 124, 125, 126
 - Ajouter une interface virtuelle personnalisée - 54
 - Confirmation de la fusion des interfaces - 132
 - Index de groupe de protocoles (rapport personnalisé) - 86
 - Index de groupe de types de service - 90
 - Index des groupes de types de service (rapport personnalisé) - 92
 - Index des types de service - 93
 - Modifier le routeur - 70
 - Modifier les interfaces - 81
 - Modifier les places réservées - 130
 - Modifier l'interface/le routeur - 70
 - Modifier une interface virtuelle personnalisée - 70

C

- CA Performance Center
 - affectation d'autorisations aux utilisateurs - 46
 - affichage de la liste des comptes d'utilisateurs - 38
 - affichage de profils SNMP - 17
 - ajout de comptes d'utilisateurs - 39
 - ajout de domaines personnalisés - 24
 - ajout de groupes personnalisés - 49
 - ajout de profils SNMP - 19
 - ajout de rôles pour les utilisateurs - 43
 - effet de l'affectation d'un client hébergé - 24
 - enregistrement de NFA - 15
 - test des connexions à la source de données - 17

-
- cFlow
 - prise en charge - 29
 - Chaîne de communauté, définition
 - définition pour l'outil de surveillance - 104
 - chaînes SNMP
 - Chaîne de communauté pour l'outil de surveillance - 104
 - changement de nom
 - routeurs - 98
 - chemins
 - journaux, chemin de configuration des journaux/services - 118
 - clients hébergés
 - effet de l'affectation - 24
 - vérification du client hébergé du Harvester - 28
 - commandes
 - configuration de NetFlow - 29
 - configuration de persistance d'index - 29
 - enregistrement de la configuration dans la mémoire statique - 29
 - composants de CA Network Flow Analysis
 - surveillance - 103
 - Composants de collecte
 - ajout d'un composant de collecte - 26
 - chaîne de communauté pour l'outil de surveillance - 104
 - modification de domaines, d'adresses, de descriptions - 75
 - présentation du rôle de collecte de données - 141
 - révision du statut de Harvester - 106
 - services/journaux installés sur les serveurs - 118
 - suppression d'un composant de collecte - 74
 - vérification du domaine/client hébergé - 28
 - configuration
 - exportation des données de systèmes autonomes vers NetFlow - 95
 - Instructions relatives à l'outil de clonage de paquets de flux - 58
 - interruptions pour les outils externes - 113
 - NetFlow, commandes - 29
 - présentation de configuration d'interruptions - 37
 - configuration matérielle requise
 - moteur pour les commutateurs Catalyst - 29
 - connexion
 - nom d'utilisateur/mot de passe par défaut - 26
 - Conserver le protocole de mappage ToS, option
 - effets sur le mappage d'applications - 122
 - Console NFA
 - avertissements - 106
 - base de données de configuration - 150
 - présentation du rôle de traitement de données - 141
 - restauration des données de configuration - 157
 - révision du statut de console - 106
 - sauvegarde de la configuration - 155
 - services/journaux installés sur les serveurs - 118
 - courriel
 - adresse pour l'outil de surveillance - 104
 - création
 - cumuls d'interfaces - 79
 - étiquettes de type de service - 90
 - filtres de temps - 99
 - groupes de protocoles - 86
 - Groupes de types de service - 91
 - interfaces virtuelles personnalisées - 54
 - interruptions - 107
 - modèles d'interface - 82
 - périodes de génération de rapports - 101
 - règles de places réservées - 129
 - cumuls d'interfaces
 - création - 79
 - effets de la suppression de routeurs - 71
 - modification - 80
 - modification de plusieurs cumuls - 81
 - suppression - 82
 - utilisations - 78
- ## D
- Définitions d'application, page
 - Mappage d'applications - 127, 128
 - Places réservées - 129, 130
 - défragmentation
 - avertissement sur la défragmentation - 158
 - démarrage
 - services, ordre de redémarrage - 155
 - dépannage
 - ajout de DSA - 32
 - problèmes avec les interruptions intégrées - 114
 - protection de l'intégrité des données - 158
 - désactivation
 - affichage des interfaces dans les rapports - 135
 - interfaces (page Interfaces actives) - 34, 133
 - rapports, par la suppression de routeurs - 71
 - surveillance générée par un routeur - 52
 - développement
-

- détails de routeur - 72
- Interfaces actives, affichage de la page - 132
- documentation
 - adresse pour les commentaires - 5
 - emplacement/liste - 4
 - Manuel de l'authentification unique - 13
- domaines
 - affichage de la liste - 23
 - ajout de domaines personnalisés - 24
 - Configuration de l'adresse ou du nom d'hôte, page - 114
 - définition du domaine de l'interface/de l'interface virtuelle personnalisée - 70
 - effets sur les valeurs de type de service - 90
 - exclusion des routeurs de l'affichage - 52
 - modification du domaine de l'interface/de l'interface virtuelle personnalisée - 70
 - modification du domaine du composant de collecte (administrateur) - 26
 - vérification du domaine du composant de collecte - 28
- données
 - architecture de collecte de données - 141
 - configuration de la collecte de flux (présentation) - 25
 - garantie de l'intégrité - 158
 - types de données collectés d'intervalle de 1 minutes - 147
 - types de données collectés d'intervalle de 15 minutes - 145
- données de configuration
 - base de données de configuration de console NFA - 150
 - conventions de fichier FlowCloneDef.ini - 60
 - emplacements de fichiers de configuration de Harvester - 150
 - enregistrement dans la mémoire statique - 29
 - exemple de fichier FlowCloneDef.ini - 59
 - fichiers de configuration pour les journaux/services - 118
 - restauration des données de configuration de console - 157
 - sauvegarde automatique - 155
 - sauvegarde manuelle des données de console - 155
- données de la présentation d'entreprise
 - base de données - 150
 - types de données/durée de stockage - 144
- données de système autonome

- modification des noms de systèmes autonomes - 97
- personnalisation des noms de système autonomes - 95
- révision des noms de systèmes autonomes - 96
- données d'historique (15 minutes)
 - emplacement de base de données - 150
 - restauration - 157
 - sauvegarde - 155
 - types de données collectées - 145
- données d'intervalle de 1 minute
 - base de données - 150
 - restauration - 157
 - sauvegarde - 155
 - types de données collectées - 147
- droits
 - affectation de droits de produit à des utilisateurs - 48

E

- enregistrement
 - source de données - 15
 - test des connexions à la source de données - 17
- étiquetage
 - valeurs de type de service - 90
- Examen des flux, page
 - définition d'emplacement/de niveau du journal - 118
 - données à partir de l'activation des interfaces - 133
- expiration
 - adresses IP expirées, motif - 114
- exportation
 - rapports sous forme de fichiers CSV, activation - 52

F

- fichiers CSV (valeurs séparées par des virgules)
 - ajout de la console aux sites de confiance - 52
- filtres de temps
 - création - 99
 - utilisation pour les interruptions - 107
- flux
 - types pris en charge - 29
- fusion
 - Confirmation de la fusion des interfaces, boîte de dialogue - 132
 - interfaces - 132

interfaces, motifs/résultats - 132

G

groupes

- ajout de groupes personnalisés (CA PC) - 49
- création de groupes de protocoles - 86
- suppression/modification par annulation d'enregistrement - 51

groupes de protocoles

- création - 86
- utilisations - 86

Groupes de types de service

- Configuration du groupe de types de service, page (administrateur) - 91
- création (administrateur) - 91
- modification du contenu (administrateur) - 93
- suppression (administrateur) - 94

groupes d'interfaces

- effets de l'annulation d'enregistrement dans CAPC - 51

H

hôtes

- Règle de mappage d'applications d'hôte - 125

I

installation

- fonctionnalité de l'outil de clonage de flux - 58
- tâches de post-installation - 52

interfaces

- activation, motifs/résultats - 133
- activation/désactivation (interfaces actives) - 133
- Confirmation de la fusion des interfaces, boîte de dialogue - 132
- définition du format de nom - 85
- désactivation de l'affichage dans les rapports - 135
- fusion - 132
- fusion, motifs/résultats - 132
- Interfaces actives, tâches de la page - 131
- modification dans la page Interfaces actives - 70
- perte lors de la suppression d'un routeur - 71
- présentation des interfaces virtuelles personnalisées - 54
- recherche dans la page Interfaces actives - 69
- standardisation des noms à l'aide de modèles - 82
- suppression - 135

vérification des interfaces surveillées - 34

vérification des vitesses, but - 52

Interfaces actives, page

- affichage des interfaces physiques et virtuelles - 66
- création/configuration des interfaces virtuelles personnalisées - 54
- fusion d'interfaces - 132
- modification des détails - 70
- personnalisation de l'apparence - 72
- présentation des tâches - 131
- recherche de routeurs/d'interfaces/d'interfaces virtuelles personnalisées - 69
- suppression de routeurs - 71
- suppression d'interfaces - 135

interfaces de bouclage

- configuration pour l'exportation NetFlow - 29

Interfaces de cumul, page

- création de cumuls - 79
- modification des cumuls - 80, 81
- suppression de cumuls - 82

Interfaces disponibles, page

- activation/désactivation des interfaces - 133
- persistance des routeurs supprimés - 71
- suppression d'interfaces des rapports - 135

interfaces virtuelles

- voir interfaces virtuelles personnalisées - 54

interfaces virtuelles personnalisées

- aperçu - 54
- création - 54
- exemple - 56
- Interfaces actives, tâches de la page - 131
- modification dans la page Interfaces actives - 70
- perte lors de la suppression d'un routeur - 71
- priorités - 56
- recherche dans la page Interfaces actives - 69
- résultats de la suppression - 54

interrogation

- délai d'expiration pour l'unité SNMP (outil de surveillance) - 104
- nouvelles tentatives pour l'unité SNMP (outil de surveillance) - 104

interruptions

- configuration pour les outils externes - 113
- création - 107
- définition de la destination (outil de surveillance) - 104
- dépannage d'interruption intégrée - 114

- Destination d'interruption, paramètre (outil de surveillance) - 104
- emplacement du fichier MIB - 113
- informations sur les interruptions, présentation - 112
- perte lors de la suppression d'un routeur - 71
- présentation de la configuration - 37
- Intervalle de contrôle du système, paramètre définition pour l'outil de surveillance - 104
- IPFIX, données
- prise en charge - 29

J

- J-Flow
- prise en charge - 29
- journaux
- noms/emplacements/fichiers de configuration des journaux - 118
- Journaux de composant de collecte
- définition d'emplacement/de niveau - 118

L

- LDAP
- pris en charge par l'outil d'authentification unique - 13
- logiciels tiers
- droits/contrats de licence - 11

M

- maintenance
- CA Network Flow Analysis - 103
- données collectées - 141
- Mappage d'applications
- aperçu - 121
- modification de règles - 127
- paramètres globaux - 122
- priorité des règles - 122
- Règle de sous-réseau - 122, 124
- Règle d'hôte - 125
- règle Tout (type de service) - 126
- suppression de règles - 128
- MIB, fichier
- accès/valeurs contenues - 113
- modèles
- modification du modèle de routeur - 70
- modification
- adresse pour le DSA actuel - 137
- adresse pour le nouveau DSA - 138

- contenu du groupe de types de service - 93
- cumuls de plusieurs interfaces - 81
- cumuls d'interfaces - 80
- Modifier le routeur, boîte de dialogue - 70, 98
- Modifier les interfaces, boîte de dialogue - 81
- Modifier les places réservées, boîte de dialogue - 130
- Modifier l'interface, boîte de dialogue - 70
- Modifier une interface virtuelle personnalisée, boîte de dialogue - 70
- nombre de détails affichés - 73
- noms de routeur - 98
- Paramètres de l'outil de surveillance - 104
- paramètres de rapport, but - 52
- règles de mappage d'applications - 127
- règles de places réservées - 130
- routeurs/interfaces (interfaces actives) - 70
- MySQL
- emplacement du service MySql51 - 118
- journal de NQMySql51 (oursql_5.1_error.log) - 118

N

- N principaux groupes
- génération de rapports sur les protocoles non N principaux - 128
- Groupes de types de service
- Configuration du groupe de types de service, page - 91
- création - 91
- modification du contenu - 93
- suppression - 94
- NetFlow
- activation de l'exportation des données de systèmes autonomes - 95
- configuration, versions prises en charge - 29
- Nfharvestererrors.log
- définition d'emplacement/de niveau - 118
- nom d'utilisateur
- connexion par défaut - 26
- Nombre maximum par page, option (interfaces actives)
- modification du nombre de détails affichés - 73
- nommage/renommage
- routeurs - 98
- valeurs de type de service - 90
- noms de DNS
- actualisation des adresses expirées - 114

notifications
des interruptions (outil de surveillance) - 104
des violations de seuil (outil de surveillance) - 104
NQMgmtSrvErrors.log
définition d'emplacement/de niveau - 118
nqservErrors.log
définition d'emplacement/de niveau - 118

O

Outil de clonage de flux
conventions de fichier de configuration - 60
exemple de configuration - 59
installation - 58
instructions relatives à la configuration - 58
paquets NetFlow - 57
restrictions relatives aux paquets IP clonés - 60
Outil de surveillance
description de services - 116
journal - 118
Paramètres de l'outil de surveillance, page - 104

P

Paramètres de l'application, page
Afficher le nom de l'unité, option - 85
password
connexion par défaut - 26
performances
ajustement des paramètres de rapport - 52
périodes de génération de rapports
création - 101
motifs de la création - 101
Périphériques SNMP
Délai d'expiration SNMP, paramètre (outil de surveillance) - 104
Nouvelles tentatives SNMP, paramètre (outil de surveillance) - 104
persistance d'index
configuration des routeurs - 29
personnalisation
apparence de la page Interfaces actives - 72
CA Network Flow Analysis - 77
Places réservées
création de règles - 129
modification de règles - 130
suppression de règles - 130
utilisation - 128
Pompage de l'émission ou de la multidiffusion

désactivation de la surveillance de routeur - 52
Port de redirection TCP, option
effets sur le mappage d'applications - 122
Port de redirection UDP, option
effets sur le mappage d'applications - 122
ports
génération de rapports avec places réservées - 129
modification pour des routeurs - 70
paramètres du port d'écoute de Harvester/d'écouteur de flux correspondant - 29
priorités
noms d'unité/d'interface - 82
Priorités de l'interface virtuelle personnalisée - 56
règle de mappage d'applications, priorités - 122
Profils SNMP
affichage de liste dans CA PC - 17
modification du profil/de la version pour un routeur - 70
programme d'authentification unique
brève description - 13
informations pour l'enregistrement dans CA PC - 15
protocoles
création d'interruptions - 107
génération de rapports avec places réservées - 129

R

rapports
activation de l'exportation au format CSV - 52
création de filtres de temps - 99
création de groupes de protocoles - 86
création de groupes de types de service - 91
création de périodes de génération de rapports - 101
création d'étiquettes de types de service - 90
protocoles/ports - 128
suppression d'interfaces - 135
Rapports d'analyse
boîte de dialogue affichant les groupes de types de service - 91
création de filtres de temps - 99
création de groupes de types de service - 91
rapports de page d'interface
création de filtres de temps - 99

- création de périodes de génération de rapports - 101
- types de rapport avec des périodes de génération de rapports - 101
- rapports personnalisés
 - boîte de dialogue affichant les groupes de types de service - 91
 - création de filtres de temps - 99
 - création de groupes de protocoles - 86
 - création de groupes de types de service - 91
 - désactivation par suppression de routeurs - 71
- RealtimeReaperErrors.log
 - définition d'emplacement/de niveau - 118
- recherche
 - de routeurs/d'interfaces (interfaces actives) - 69
- redémarrage
 - services, ordre de redémarrage - 155
- règles
 - Places réservées, création - 129
 - Places réservées, présentation - 128
 - Règle de mappage d'applications de sous-réseau - 122, 124
 - Règle de mappage d'applications d'hôte - 125
 - règle de mappage d'applications Tout (type de service) - 126
 - règle de mappage d'applications, priorités - 122
- restauration
 - bases de données - 157
- rôles
 - ajout pour les utilisateurs - 43
- routeurs
 - activation de NetFlow - 29
 - configuration - 29
 - configuration de la persistance d'index - 29
 - désactivation de la surveillance - paramètre - 52
 - développement des détails - 72
 - Interfaces actives, tâches de la page - 131
 - modification des détails - 70
 - modification du nombre de détails affichés - 73
 - motifs pour le renommage/renommage - 98
 - recherche dans la page Interfaces actives - 69
 - routeurs - 98
 - suppression des interfaces actives - 71

S

- sauvegarde
 - bases de données - 155
- Serveur de gestion

- journal (NQMgmtSrvErrors) - 118
- Service de base d'informations de génération de rapports
 - emplacement du journal de service de base d'informations de génération de rapports de CA NFA - 118
- Service de génération de rapports
 - description - 116
 - noms/emplacements des journaux - 118
- Service de gestionnaire
 - description - 116
 - journal - 118
- Service de pompage
 - description - 116
 - journal (PumpLog.log) - 118
- Service de rapport
 - journal (FlowForensicsLog.log) - 118
- services
 - brève description - 116
 - emplacements/journaux/fichiers de configuration - 118
- Services de requête
 - définition d'emplacement/de niveau du journal - 118
- Services généraux
 - description - 116
 - journal (nqservErrors) - 118
- Seuil de disque, paramètre
 - définition pour l'outil de surveillance - 104
- Seuil de mémoire, paramètre
 - définition pour l'outil de surveillance - 104
- Seuil d'UC, définition
 - définition pour l'outil de surveillance - 104
- seuils
 - création pour les interruptions - 107
 - définition pour les interruptions/alertes NFA - 107
 - notifications (outil de surveillance) - 104
 - seuil de disque pour l'outil de surveillance - 104
 - Seuil d'UC pour l'outil de surveillance - 104
 - Utilisation de la mémoire (outil de surveillance) - 104
- sFlow
 - version prise en charge - 29
- sous-réseaux
 - modification de la description de l'interface virtuelle personnalisée - 70
 - Règle de mappage d'applications de sous-réseau - 122, 124

- status
 - vérification des statuts de composant - 106
- Statut du système, page
 - ouverture/utilisation - 61
- soutien technique
 - Portail de self-service de CA - 5
- suppression
 - cumuls d'interfaces - 82
 - groupes de protocoles - 86
 - Groupes de types de service - 94
 - groupes/utilisateurs par annulation d'enregistrement - 51
 - interfaces - 135
 - protocoles d'un groupe - 86
 - règles de mappage d'applications - 128
 - règles de places réservées - 130
 - résultats pour les interfaces virtuelles personnalisées - 54
 - routeurs, des interfaces actives - 71
- surveillance
 - composants - 103

T

- tables
 - tri - 72
- test
 - connexion à la source de données - 17
- tri
 - lignes de table - 72
- Type de service
 - création d'interruptions - 107
 - effets du masque de type de service sur le mappage d'applications - 122
 - étiquettes de type de service, création - 90
 - Index des types de service, boîte de dialogue - 93
 - règle de mappage d'applications Tout (type de service) - 126

U

- utilisateurs
 - affectation d'autorisations - 46
 - affectation de droits de produit - 48
 - affichage de la liste des comptes d'utilisateurs - 38
 - ajout de comptes d'utilisateurs - 39
 - ajout de rôles - 43
 - création de comptes d'utilisateurs, but - 52
 - suppression par annulation d'enregistrement - 51

- Utilisation de la mémoire
 - modification du seuil de l'outil de surveillance - 104

V

- vérification
 - domaine du composant de collecte - 28
 - interfaces activées - 34
 - statut de composant - 106
 - visibilité d'interface (console NFA) - 35
 - vitesse des interfaces, but - 52
- vérification du domaine du composant de collecte - 28
 - domaine du composant de collecte - 28
- vitesse en entrée/en sortie
 - modification d'interfaces/d'interfaces virtuelles personnalisées - 70
- volume
 - génération de rapports sur les protocoles à faible volume - 129